π-adic approach of p-class group and unit group of p-cyclotomic fields

Roland Quême

2005 fev 04

Contents

Abstract

Roland Quême
13 avenue du château d'eau
31490 Brax
France
2005 fev 04
tel : 0033561067020
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/
Mathematical subject classification: Primary 11R18, Secondary 11R27, 11R29
****

Let $p > 2$ be a prime. Let $\mathbb{Q}(\zeta)$ be the p-cyclotomic field. Let $\mathbb{Q}(\zeta)^+$ be its maximal totally real subfield. Let π be the prime ideal of $\mathbb{Q}(\zeta)$ lying over p. This articles aims to describe some π-adic congruences characterising the structure of the p-class group and of the p-unit group of the fields $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta)^+$. For the unit group, this paper supplements the papers of Dénes of 1954 and 1956. A complete summarizing of the results obtained in the paper follows in the *Introduction section* 1 from p. 3 to 6 . This paper is at elementary level.

1 Introduction

Let $p > 2$ be a prime. Let $\mathbb{Q}(\zeta)$ be the p-cyclotomic fields. Let $\mathbb{Z}[\zeta]$ be the ring of integers of $\mathbb{Q}(\zeta)$. Let $\pi = (1-\zeta)\mathbb{Z}[\zeta]$ be the prime ideal of $\mathbb{Q}(\zeta)$ lying over p. This monograph contains two parts:

1. a description of π-adic congruences strongly connected to p-class group of $\mathbb{Q}(\zeta)$ and its structure.

2. a description of π-adic congruences on p-unit group of $\mathbb{Q}(\zeta)$.

1.1 Some π-adic congruences connected to p-class group of cyclotomic field $\mathbb{Q}(\zeta)$

This topic is studied in section 3 p. 9 of this paper. Let us give at first some definitions:

1. Let p be an odd prime. Let ζ be a root of the equation $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. Let $\mathbb{Q}(\zeta)$ be the p-cyclotomic field and $\mathbb{Z}[\zeta]$ be the ring of integers of $\mathbb{Q}(\zeta)$.

2. Let $\sigma : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta)$ be a $\mathbb{Q}$-isomorphism of the field $\mathbb{Q}(\zeta)$ generating the cyclic Galois group $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. There exists $u \in \mathbb{N}$, primitive root $\mod p$, such that $\sigma(\zeta) = \zeta^u$.

3. Let C_p, C_p^+, C_p^- be respectively the subgroups of exponent p of the p-class group of $\mathbb{Q}(\zeta)$, of the p-class group of $\mathbb{Q}(\zeta + \zeta^{-1})$ and the relative p-class group $C_p^- = C_p/C_p^+$. Let r_p, r_p^+, r_p^- be respectively the p-rank of C_p, C_p^+, C_p^-, seen as $\mathbf{F}_p[G]$ modules.

4. It is possible to write C_p in the form $C_p = \oplus_{i=1}^{r_p} \Gamma_i$, where Γ_i is a cyclic group of order p, subgroup globally invariant under the action of the Galois group G.

5. Let $\mathbf{b}_i, \quad i = 1, \dots, r_p$, be a not principal integral ideal of $\mathbb{Q}(\zeta)$ whose class belongs to the group Γ_i. Observe at first that $\mathbf{b}_i^p$ is principal and that $\sigma(\mathbf{b}_i) \simeq \mathbf{b}_i^{\mu_i}$ where $\simeq$ is notation for class equivalence and $\mu_i \in \mathbf{F}_p^*$ with $\mathbf{F}_p^*$ the set of $p-1$ no null elements of the finite field of cardinal p. Let the ideal $\mathbf{b} = \prod_{i=1}^{r_p} \mathbf{b}_i$, which generates C_p under action of the group G.

6. A number $a \in \mathbb{Q}(\zeta)$ is said *singular* if there exists a not principal ideal $\mathbf{a}$ of $\mathbb{Q}(\zeta)$ such that $a\mathbb{Z}[\zeta] = \mathbf{a}^p$. A singular number $a \in \mathbb{Q}(\zeta)$ is said *primary* if there exists $\alpha \in \mathbb{N}, \quad \alpha \not\equiv 0 \mod p$ such that $a \equiv \alpha^p \mod \pi^p$.

7. Let $d \in \mathbb{N}, \quad p-1 \equiv 0 \mod d$. Let G_d be the subgroup of order $\frac{p-1}{d}$ of the Galois group G. Let us define the minimal polynomial $P_{r_d}(X)$ of degree r_d in the indeterminate X, where $P_{r_d}(\sigma^d) \in \mathbf{F}_p[G_d]$ annihilates the ideal class of $\mathbf{b}$, written also $\mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]$. The polynomial $P_{r_d}(\sigma^d)$ is of form $P_{r_d}(\sigma^d) = \prod_{i=1}^{r_d}(\sigma^d - \mu_i^d), \quad \mu_i \in \mathbf{F}_p^*$. When $d = 1$, then $G_d = G$, Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q})$, and $r_d = r_1$. Note that if $d > 1$ then $r_d \leq r_1$.

We obtain the following results:

1. For d_1, d_2 co-prime natural integers with $d_1 \times d_2 = p-1$, the degrees in the indeterminate X of minimal polynomials $P_{r_{d_1}}(X)$ and $P_{r_{d_2}}(X)$ verify: if $r_{d_1} \geq 1$ and $r_{d_2} \geq 1$ then $r_{d_1} \times r_{d_2} \geq r_1$.

2. Let us set $d = 1$. Let us note $r_1 = r_1^+ + r_1^-$, where r_1^+ and r_1^- are respectively the degrees of the minimal polynomials $P_{r_1^+}(\sigma)$ and $P_{r_1^-}(\sigma)$, corresponding to annihilation of groups C_p^+ and C_p^- with $C_p = C_p^+ \oplus C_p^-$. The following result connects strongly the degree r_1^- to Bernoulli Numbers: the degree r_1^- is the index of irregularity of $\mathbb{Q}(\zeta)$ (the number of even Bernoulli Numbers $B_{p-1-2m} \equiv 0 \mod p$ for $1 \leq m \leq \frac{p-3}{2}$). Moreover the degree r_1^- verifies the inequality $r_p^- - r_p^+ \leq r_1^- \leq r_p^-$.

3. Let the ideal $\pi = (\zeta - 1)\mathbb{Z}[\zeta]$. The following results are π-adic congruences strongly connected to structure of p-class group C_p of $\mathbb{Q}(\zeta)$:

   (a) There exists singular algebraic integers $B_i \in \mathbb{Z}[\zeta] - \mathbb{Z}[\zeta]^*, \quad i = 1, \dots, r_p$, verifying:

      i. $B_i\mathbb{Z}[\zeta] = \mathbf{b}_i^p$ with $\mathbf{b}_i$ defined above

      ii. $\sigma(\mathbf{b}_i) \simeq \mathbf{b}_i^{\mu_i}$.

      iii. $\sigma(B_i) = B_i^{\mu_i} \times \alpha_i^p, \quad \alpha_i \in \mathbb{Q}(\zeta), \quad \mu_i \in \mathbf{F}_p^*$.

      iv. $\sigma(B_i) \equiv B_i^{\mu_i} \mod \pi^p$.

      v. For the value $m_i \in \mathbb{N}$ verifying $\mu_i = u^{m_i} \mod p, \quad 1 \leq m_i \leq p-2$, then
      $$\pi^{m_i} \mid B_i - 1.$$

   (b) We can precise the previous result: with it a certain reordering of indexing of $B_i, \quad i = 1, \dots, r_p$,

      i. For $i = 1, \dots, r_p^+$, then the B_i are *primary*, so $\pi^p \mid B_i - 1$.

      ii. For $i = r_p^+ + 1, \dots, r_p^-$, then the B_i are *not primary.* They verify the congruence
      $$\pi^{m_i} \parallel B_i - 1.$$

iii. For $i = r_p^- + 1, \dots, r_p$, then the B_i are *primary or not primary* (without being able to have a more precise result) with

$$\pi^{m_i} \mid B_i - 1.$$

(c) Let $\mu_i = u^{2m_i+1} \bmod p$ with $1 \leq m_i \leq \frac{p-3}{2}$ corresponding to an ideal $\mathbf{b}_i$ whose class belongs to C_p^-, relative p-class group of $\mathbb{Q}(\zeta)$. In that case define $C_i = \frac{B_i}{\overline{B}_i}$ with B_i already defined, so with $C_i \in \mathbb{Q}(\zeta)$. If $2m_i+1 > \frac{p-1}{2}$ then it is possible to prove the explicit very straightforward formula for $C_i \bmod \pi^{p-1}$:

$$C_i \equiv 1 - \frac{\gamma_{p-3}}{1-\mu_i} \times (\zeta + \mu_i^{-1}\zeta^u + \dots + \mu_i^{-(p-2)}\zeta^{u^{p-2}}) \bmod \pi^{p-1}, \quad \gamma_{p-3} \in \mathbf{F}_p^*.$$

1.2 Some π-adic congruences on p-unit group the cyclotomic field

This topic is studied in section 4 p. 34. We apply in following results to unit group $\mathbb{Z}[\zeta + \zeta^{-1}]^*$ the method applied to p-class group in previous results:

1. There exists a fundamental system of units $\eta_i, \quad i = 1, \dots, \frac{p-3}{2}$, of the group $F = \{\mathbb{Z}[\zeta + \zeta^{-1}]^* / (\mathbb{Z}[\zeta + \zeta^{-1}]^*)^p\} / < -1 >$ verifying the relations:

$$(1) \qquad \begin{aligned} &\eta_i \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \quad i = 1, \dots, \frac{p-3}{2}, \\ &\sigma(\eta_i) = \eta_i^{\mu_i} \times \varepsilon_i^p, \\ &\varepsilon_i \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \\ &n_i \in \mathbb{N}, \text{ with } \mu_i = u^{2n_i} \bmod p, \quad 1 \leq n_i \leq \frac{p-3}{2}, \\ &\eta_i \equiv 1 \bmod \pi^{2n_i}, \quad i = 1, \dots, \frac{p-3}{2}, \\ &\sigma(\eta_i) \equiv \eta_i^{\mu_i} \bmod \pi^{p+1}, \quad i = 1, \dots, \frac{p-3}{2}. \end{aligned}$$

2. With a *certain reordering of indexing* of $i = 1, \dots, \frac{p-3}{2}$,

   (a) For $i = 1, \dots, r_p^+$ then η_i are *not primary units* and

   $$\pi^{2n_i} \parallel \eta_i - 1.$$

   (b) For $i = r_p^+ + 1, \dots, r_p^-$, then η_i are *primary units* and

   $$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i > 0.$$

(c) For $i = r_p^- + 1, \ldots, r_p$, then η_i are *not primary or primary units* and

$$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i \geq 0.$$

(d) For $i = r_p + 1, \ldots, \frac{p-3}{2}$, then η_i are *not primary units* and

$$\pi^{2n_i} \parallel (\eta_i - 1).$$

3. If $2n_i > \frac{p-1}{2}$ then it is possible to prove the very straightforward explicit formula for η_i:

$$\eta_i \equiv 1 - \frac{\gamma_{p-3}}{1-\mu_i} \times (\zeta + \mu_i^{-1}\zeta^u + \cdots + \mu_i^{-(p-2)}\zeta^{u^{p-2}}) \bmod \pi^{p-1}, \quad \gamma_{p-3} \in \mathbf{F}_p^*.$$

2 Cyclotomic Fields : some definitions

In this section, we fix notations used in all this paper.

- For $a \in \mathbb{R}^+$, we note $[a]$ the integer part of a or the integer immediately below a.
- We denote $[a, b], \quad a, b \in \mathbb{R}$, the closed interval bounded by a, b.
- Let us denote $< a >$ the cyclic group generated by the element a.
- Let $p \in \mathbb{N}$ be an odd prime.
- Let $\mathbb{Q}(\zeta_p)$, or more brievely $\mathbb{Q}(\zeta)$ when there is no ambiguity of the context, be the p-cyclotomic number field.
- Let $\mathbb{Z}[\zeta]$ be the ring of integers of $\mathbb{Q}(\zeta)$.
- Let $\mathbb{Z}[\zeta]^*$ be the group of units of $\mathbb{Z}[\zeta]$.
- Let $\mathbb{Q}(\zeta+\zeta^{-1})$ be the maximal real subfield of $\mathbb{Q}(\zeta)$, with $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta+\zeta^{-1})] = 2$. The ring of integers of $\mathbb{Q}(\zeta + \zeta^{-1})$ is $\mathbb{Z}[\zeta + \zeta^{-1}]$. Let $\mathbb{Z}[\zeta + \zeta^{-1}]^*$ be the group of units of $\mathbb{Z}[\zeta + \zeta^{-1}]$.
- Let $\mathbf{F}_p$ be the finite field with p elements. Let $\mathbf{F}_p^* = \mathbf{F}_p - \{0\}$.
- Let us denote $\mathbf{a}$ the integral ideals of $\mathbb{Z}[\zeta]$. Let us note $\mathbf{a} \simeq \mathbf{b}$ when the two ideals $\mathbf{a}$ and $\mathbf{b}$ are in the same class of the class group of $\mathbb{Q}(\zeta)$. The relation $\mathbf{a} \simeq \mathbb{Z}[\zeta]$ means that the ideal $\mathbf{a}$ is principal.
- Let us note $Cl(\mathbf{a})$ the class of the ideal $\mathbf{a}$ in the class group of $\mathbb{Q}(\zeta)$. Le us note $< Cl(\mathbf{a}) >$ the finite group generated by the class $Cl(\mathbf{a})$.
- If $a \in \mathbb{Z}[\zeta]$, we note $a\mathbb{Z}[\zeta]$ the principal integral ideal of $\mathbb{Z}[\zeta]$ generated by a.
- We have $p\mathbb{Z}[\zeta] = \pi^{p-1}$ where π is the principal prime ideal $(1 - \zeta)\mathbb{Z}[\zeta]$. Let us denote $\lambda = \zeta - 1$, so $\pi = \lambda\mathbb{Z}[\zeta]$.
- Let $G = Gal(\mathbb{Q}(\zeta/\mathbb{Q})$ be the Galois group of the field $\mathbb{Q}(\zeta)$. Let $\sigma : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta)$ be a $\mathbb{Q}(\zeta)$-isomorphism generating the cyclic group G. The $\mathbb{Q}$-isomorphism σ can be defined by $\sigma(\zeta) = \zeta^u$ where u is a primitive root $\mod p$.
- For this primitive root u mod p and $i \in \mathbb{N}$, let us denote $u_i \equiv u^i \mod p, \quad 1 \leq u_i \leq p - 1$. For $i \in \mathbb{Z}, \quad i < 0$, this is to be understood as $u_i u^{-i} \equiv 1 \mod p$. This notation follows the convention adopted in Ribenboim [6], last paragraph of page 118. This notation is largely used in the sequel of this monograph.

- For $d \in \mathbb{N}, \quad p-1 \equiv 0 \bmod d$, let G_d be the cyclic subgroup of G of order $\frac{p-1}{d}$ generated by σ^d, so with $G_1 = G$. The group G_d is the Galois group of the extension $\mathbb{Q}(\zeta)/K_d$ where K_d is a field with $\mathbb{Q} \subset K_d \subset \mathbb{Q}(\zeta)$ and $[K_d : \mathbb{Q}] = d$.

- Let C_p be the subgroup of exponent p of the p-class group of the field $\mathbb{Q}(\zeta)$.

- Let C_p^+ be the subgroup of exponent p of the p-class group of the field $\mathbb{Q}(\zeta+\zeta^{-1})$.

- Let C_p^- be the relative class group defined by $C_p^- = C_p/C_p^+$.

- Let h be the class number of $\mathbb{Q}(\zeta)$. The class number h verifies the formula $h = h^- \times h^+$, where h^+ is the class number of the maximal real field $\mathbb{Q}(\zeta+\zeta^{-1})$, so called also second factor, and h^- is the relative class number, so called first factor.

- Let us define respectively e_p, e_p^-, e_p^+ by $h = p^{e_p} \times h_2, \quad h_2 \not\equiv 0 \bmod p$, by $h^- = p^{e_p^-} \times h_2^-, \quad h_2^- \not\equiv 0 \bmod p$ and by $h^+ = p^{e_p^+} \times h_2^+, \quad h_2^+ \not\equiv 0 \bmod p$

- Let r_p, r_p^+, r_p^-, be respectively the p-rank of the p-class group of $\mathbb{Q}(\zeta)$, of the p-class group of $\mathbb{Q}(\zeta+\zeta^{-1})$ and of the relative class group seen as $\mathbf{F}_p[G]$-modules, so with $r_p \leq e_p, \quad r_p^+ \leq e_p^+$ and $r_p^- \leq e_p^-$.

- The abelian group C_p is a group of order p^{r_p} with $C_p = \oplus_{i=1}^{r_p} C_i$ where C_i are cyclic group of order p.

3 π-adic congruences on p-subgroup C_p of the class group of $\mathbb{Q}(\zeta)$

- The two first subsections 3.1 p.9 and 3.2 p.10 give some definitions, notations and general classical properties of the p-class group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. **They can be omitted at first** and only looked at for fixing notations.

- In subsection 3.3 p. 14, we get several results on the structure of the p-class group C_p of $\mathbb{Q}(\zeta)$ and on class number h of $\mathbb{Q}(\zeta)$:

  - A formulation, with our notations, of a Ribet's result on irregularity index.
  - Let $d, g \in \mathbb{N}$ coprime with $d \times g = p - 1$. For groups generated by the action of Galois groups G and of subgroups G_d, G_g of G on ideals $\mathbf{b}$ of $\mathbb{Q}(\zeta)$, an inequality between degrees r_1, r_d, r_g of minimal polynomials $P_{r_1}(\sigma) \in \mathbf{F}_p[G], \quad P_{r_d}(\sigma^d) \in \mathbf{F}_p[G_d], \quad P_{r_g}(\sigma^g) \in \mathbf{F}_p[G_g]$ annihilating ideal class of $\mathbf{b}$.
  - Some π-adic congruences connected to structure of p-class group C_p of $\mathbb{Q}(\zeta)$.

3.1 Some definitions and notations

In this subsection, we fix or recall some notations used in all this section.

- Let G be the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$. Let $d \in \mathbb{N}, \quad p - 1 \equiv 0 \mod d$. Let G_d be the subgroup of the cyclic group G. Then G_d is of order $\frac{p-1}{d}$. If σ generates G, then σ^d generates G_d.

- Let $\mathbf{b}$ be an ideal of $\mathbb{Z}[\zeta]$, not principal and with $\mathbf{b}^p$ principal.

- Let $c_i = Cl(\sigma^i(\mathbf{b})), \quad i = 0, \dots, p-2$, be the class of $\sigma^i(\mathbf{b})$ in the p-class group of $\mathbb{Q}(\zeta)$.

- Recall that $Cl(\mathbf{b})$ is the class of the ideal $\mathbf{b}$ of $\mathbb{Z}[\zeta]$. Observe that exponential notations $\mathbf{b}^\sigma$ can be used indifferently in the sequel. With this notation, we have

  - $\mathbf{b}^{\sigma^d} = \sigma^d(\mathbf{b})$.
  - For $\lambda \in \mathbf{F}_p$, we have $\mathbf{b}^{\sigma+\lambda} = \mathbf{b}^\lambda \times \sigma(\mathbf{b})$.
  - Let $P(\sigma) = \sigma^m + \lambda_{m-1}\sigma^{m-1} + \dots + \lambda_1\sigma + \lambda_0 \in \mathbf{F}_p[\sigma]$; then $\mathbf{b}^{P(\sigma)} = \sigma^m(\mathbf{b}) \times \sigma^{m-1}(\mathbf{b})^{\lambda_{m-1}} \times \dots \times \sigma(\mathbf{b})^{\lambda_1} \times \mathbf{b}^{\lambda_0}$.

- Let us note $\mathbf{b}^{P(\sigma)} \simeq \mathbb{Z}[\zeta]$, if the ideal $\sigma^m(\mathbf{b})\times\sigma^{m-1}(\mathbf{b})^{\lambda_{m-1}}\dots\sigma(\mathbf{b})^{\lambda_1}\times\mathbf{b}^{\lambda_0}$ is principal.
- Let $P(\sigma), Q(\sigma) \in \mathbf{F}_p[\sigma]$; if $\mathbf{b}^{P(\sigma)} \simeq \mathbb{Z}[\zeta]$, then $\mathbf{b}^{Q(\sigma)\times P(\sigma)} \simeq \mathbb{Z}[\zeta]$.
- Observe that trivially $\mathbf{b}^{\sigma^{p-1}-1} \simeq \mathbb{Z}[\zeta]$.

- There exists a monic minimal polynomial $P_{r_d}(V) \in \mathbf{F}_p[V]$, polynomial ring of the indeterminate V verifying the relation, for $V = \sigma^d$:

$$\mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]. \tag{2}$$

  This minimality implies that, for all polynomials $R(V) \in \mathbf{F}_p(V), \quad R(V) \neq 0, \quad deg(R(V)) < deg(P_{r_d}(V))$, we have $\mathbf{b}^{R(\sigma^d)} \not\simeq \mathbb{Z}[\zeta]$. It means, with an other formulation in term of ideals, that $\prod_{i=0}^{r_d}\sigma^{id}(\mathbf{b})^{\lambda_{i,d}}$ is a principal ideal and that $\prod_{i=0}^{\alpha}\sigma^{id}(\mathbf{b})^{\beta_i}$ is not principal when $\alpha < r_d$ and $\beta_i, \quad i = 0,\dots,\alpha$, are not all simultaneously null.

- $P_{r_d}(U)$ is the **minimal polynomial** of the indeterminate U with $P_{r_d}(\sigma^d) \in \mathbf{F}_p[G_d]$ **annihilating** the ideal class of $\mathbf{b}$.

3.2 Representations of Galois group $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ in characteristic p.

In this subsection we give some general properties of representations of $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ in characteristic p and obtain some results on the structure of the p-class group of $\mathbb{Q}(\zeta)$. Observe that we never use characters theory.

Lemma 3.1. *Let $d \in \mathbb{N}, \quad p-1 \equiv 0 \mod d$. Let V be an indeterminate. Then the minimal polynomial $P_{r_d}(V)$ with $P_{r_d}(\sigma^d) \in \mathbf{F}_p[G_d]$ annihilating ideal class of* $\mathbf{b}$ *verifies the factorization*

$$P_{r_d}(V) = \prod_{i=1}^{r_d}(V - \mu_{i,d}), \quad \mu_{i,d} \in \mathbf{F}_p, \quad i_1 \neq i_2 \Rightarrow \mu_{i_1} \neq \mu_{i_2}.$$

Proof. Let us consider the polynomials $A(V) = V^{p-1} - 1$ and $P_{r_d}(V) \in \mathbf{F}_p[V]$. It is possible to divide the polynomial $A(V)$ by $P_{r_d}(V)$ in the polynomial ring $\mathbf{F}_p[V]$ to obtain

$$A(V) = P_{r_d}(V) \times Q(V) + R(V), \quad Q(V), R(V) \in \mathbf{F}_p[V],$$
$$d_R = deg_V(R(V)) < r_d = deg_V(P_{r_d}(V)).$$

For $V=\sigma^d$, we get $\mathbf{b}^{\sigma^{d(p-1)}-1}\simeq \mathbb{Z}[\zeta]$ and $\mathbf{b}^{P_{r_d}(\sigma^d)}\simeq \mathbb{Z}[\zeta]$, so $\mathbf{s}^{R(\sigma^d)}\simeq \mathbb{Z}[\zeta]$. Suppose that $R(V)=\sum_{i=0}^{d_R} R_i V^i,\quad R_i\in \mathbf{F}_p$, is not identically null; then, it leads to the relation

$$\sum_{i=0}^{d_R} R_i\sigma^{di}(\mathbf{b})\simeq \mathbb{Z}[\zeta],$$

where the R_i are not all zero, with $d_R<r_d$, which contradicts the minimality of the polynomial $P_{r_d}(V)$. Therefore, $R(V)$ is identically null and we have

$$V^{p-1}-1=P_{r_d}(V)\times Q(V).$$

The factorization of $V^{p-1}-1$ in $\mathbf{F}_p[V]$ is $V^{p-1}-1=\prod_{i=1}^{p-1}(V-i)$. The factorization is unique in the euclidean ring $\mathbf{F}_p[V]$ and so $P_{r_d}(V)=\prod_{i=1}^{r_d}(V-\mu_{i,d}),\quad \mu_{i,d}\in \mathbf{F}_p,\quad i_1\neq i_2\Rightarrow \mu_{i_1}\neq\mu_{i_2}$, which achieves the proof. □

****

Lemma 3.2. *Let $d\in\mathbb{N},\quad p-1\equiv 0 \bmod d$. Let U,W be two indeterminates. Let $P_{r_1}(U)$ be the minimal polynomial with $P_{r_1}(\sigma)\in\mathbf{F}_p[G]$ annihilating the ideal class of $\mathbf{b}$. Let $P_{r_d}(W)$ be the minimal polynomial with $P_{r_d}(\sigma^d)\in\mathbf{F}_p[G_d]$ annihilating the ideal class of $\mathbf{b}$. Then*

1. $P_{r_1}(U)=\prod_{i=1}^{r_1}(U-\mu_i),\quad \mu_i\in\mathbf{F}_p$.
2. $P_{r_d}(U^d)=\prod_{i=1}^{r_d}(U^d-\mu_i^d)=P_{r_1}(U)\times Q_d(U),\quad r_d\leq r_1,\quad Q_d(U)\in\mathbf{F}_p[U]$.
3. *The p-ranks r_1 and r_d verify the inequalities*

$$r_d\times d\geq r_1\geq r_d. \tag{3}$$

4. *Let K_d be the intermediate field $\mathbb{Q}\subset K_d\subset\mathbb{Q}(\zeta),\quad [K_d:\mathbb{Q}]=d$. Suppose that p does not divide the class number of $K_d/\mathbb{Q}$; then $\mu_i^d\neq 1$ for $i=1,\dots,r_d$. In particular $\mu_i\neq 1$ for $i=1,\dots,r_1$.*

Proof.

- Observe, at first, that $deg_U(P_{r_d}(U^d))=d\times r_d\geq r_1$: if not, for the polynomial $P_{r_d}(U^d)$ seen in the indeterminate U, whe should have $deg_U(P_{r_d}(U^d))<r_1$ and $P_{r_d}(\sigma^d)\circ\mathbf{b}\simeq\mathbb{Z}[\zeta]$ and, as previously, the polynomial $P_{r_d}(U^d)$ of the indeterminate U should be identically null.
- We apply euclidean algorithm in the polynomial ring $\mathbf{F}_p[U]$ of the indeterminate U. Therefore,

$$P_{r_d}(U^d)=P_{r_1}(U)\times Q(U)+R(U),\quad Q(U),R(U)\in\mathbf{F}_p[U],$$
$$deg(R(U))<deg(P_{r_1}(U)).$$

But we have $\mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta], \quad \mathbf{b}^{P_{r_1}(\sigma)} \simeq \mathbb{Z}[\zeta]$, therefore $\mathbf{b}^{R(\sigma)} \simeq \mathbb{Z}[\zeta]$. Then, similarly to proof of lemma 3.1 p.10, $R(U)$ is identically null and $P_{r_d}(U^d) = P_{r_1}(U) \times Q(U)$.

- Applying lemma 3.1 p.10, we obtain

$$P_{r_1}(U) = \prod_{i=1}^{r_1}(U - \mu_i), \quad \mu_i \in \mathbf{F}_p,$$
$$P_{r_d}(U^d) = \prod_{i=1}^{r_d}(U^d - \mu_{i,d}), \quad \mu_{i,d} \in \mathbf{F}_p.$$

- Then, we get

$$P_{r_d}(U^d) = \prod_{i=1}^{r_d}(U^d - \mu_{i,d}) = \prod_{i=1}^{r_1}(U - \mu_i) \times Q(U).$$

There exists at least one $i, \quad 1 \le i \le r_d$, such that $(U^d - \mu_{i,d}) = (U - \mu_1) \times Q_1(U)$: if not, for all $i = 1, \dots, r_d$, we should have $U^d - \mu_{i,d} \equiv R_i \mod (U - \mu_1), \quad R_i \in \mathbf{F}_p^*$, a contradiction because $\prod_{i=1}^{r_d} R_i \ne 0$. We have $\mu_{i,d} = \mu_1^d$: if not $U - \mu_1$ should divide $U^d - \mu_{i,d}$ and $U^d - \mu_1^d$ and also $U - \mu_1$ should divide $(\mu_{i,d} - \mu_1^d) \in \mathbf{F}_p^*$, a contradiction. Therefore, there exists at least one $i, \quad 1 \le i \le r_d$, such that $\mu_{i,d} = \mu_1^d$ and $U^d - \mu_{i,d} = U^d - \mu_1^d = (U - \mu_1) \times Q_1(U)$.

Then, generalizing to $\mu_{i,d}$ for all $i = 1, \dots, r_d$, we get with a certain reordering of index i

$$P_{r_d}(U^d) = \prod_{i=1}^{r_d}(U^d - \mu_i^d) = \prod_{i=1}^{r_1}(U - \mu_i) \times Q(U).$$

- We have

$$P_{r_d}(U^d) = \prod_{i=1}^{r_d}(U^d - \mu_i^d).$$

This relation leads to

$$P_{r_d}(U^d) = \prod_{i=1}^{r_d}\prod_{j=1}^{d}(U - \mu_i \mu_d^j),$$

where $\mu_d \in \mathbf{F}_p, \quad \mu_d^d = 1$. We have shown that $P_{r_d}(U^d) = P_{r_1}(U) \times Q_d(U)$ and so $deg_U(P_{r_d}(U)) = d \times r_d \ge r_1$; thus $d \times r_d \ge r_1$.

- We finish by the proof of item 4): suppose that, for some i, $1 \leq i \leq r_d$, we have $\mu_i^d = 1$ and search for a contradiction: there exists, for the indeterminate V, a polynomial $P_1(V) \in \mathbf{F}_p(V)$ such that $P_{r_d}(V) = (V - \mu_i^d) \times P_1(V) = (V-1) \times P_1(V)$. But for $V = \sigma^d$, we have $\mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]$, so $\mathbf{b}^{(\sigma^d P_1(\sigma^d) - P_1(\sigma^d))} \simeq \mathbb{Z}[\zeta]$. So, $\mathbf{b}^{P_1(\sigma^d)}$ is the class of an ideal $\mathbf{c}$ of $\mathbb{Z}[\zeta]$ with $Cl(\sigma^d(\mathbf{c})) = Cl(\mathbf{c})$; then $Cl(\sigma^{2d}(\mathbf{c})) = Cl(\sigma^d(\mathbf{c})) = Cl(\mathbf{c})$. Then $Cl(\sigma^d(\mathbf{c}) \times \sigma^{2d}(\mathbf{c}) \times \cdots \times \sigma^{(p-1)d/d}(\mathbf{c})) = Cl(\mathbf{c}^{(p-1)/d})$. Let $\tau = \sigma^d$; then $Cl(\tau(\mathbf{c}) \times \tau^2(\mathbf{c}) \times \cdots \times \tau^{(p-1)/d}(\mathbf{c})) = Cl(\mathbf{c}^{(p-1)/d})$; Then we deduce that $Cl(N_{\mathbb{Q}(\zeta)/K_d}(\mathbf{c})) = Cl(\mathbf{c}^{(p-1)/d})$ and thus $\mathbf{c}$ is a principal ideal because the ideal $N_{\mathbb{Q}(\zeta)/K_d}(\mathbf{c})$ of K_d is principal, (recall that, from hypothesis, p does not divide $h(K_d/\mathbb{Q})$); so $\mathbf{b}^{P_1(\sigma^d)} \simeq \mathbb{Z}[\zeta]$, which contradicts the minimality of the minimal polynomial equation $\mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]$ because, for the indeterminate V, we would have $deg(P_1(V)) < deg(P_{r_d}(V))$, which achieves the proof.

$\square$

Remark: As an example, the item 4) says that:

1. If $d = 2$, then classically $p \not| h(K_2/\mathbb{Q})$ and so item 4) shows that $\mu_i \neq -1$: there is no ideal $\mathbf{b}$ whose class belongs to C_p which is annihilated by $\sigma - u_{(p-1)/2} = \sigma + 1$.
2. if $h^+ \not\equiv 0$ mod p, (Vandiver's conjecture) then $\mu_i^{(p-1)/2} = -1$ for $i = 1, \ldots, r_1$.

We summarize results obtained in:

Lemma 3.3. *Let* $\mathbf{b}$ *be an ideal of* $\mathbb{Z}[\zeta]$, $\mathbf{b}^p \simeq \mathbb{Z}[\zeta]$, $\mathbf{b} \not\simeq \mathbb{Z}[\zeta]$. *Let* $d \in \mathbb{N}$, $p - 1 \equiv 0$ *mod* d. *Let* U, W *be two indeterminates. Let* $P_{r_1}(U)$ *be the minimal polynomial with* $P_{r_1}(\sigma) \in \mathbf{F}_p[G]$ *annihilating the ideal class of* $\mathbf{b}$. *Let* $P_{r_d}(W)$ *be the minimal polynomial with* $P_{r_d}(\sigma^d) \in \mathbf{F}_p[G_d]$ *annihilating the ideal class of* $\mathbf{b}$. *Then there exists* $\mu_1, \mu_2, \ldots, \mu_{r_1} \in \mathbf{F}_p$, *with* $i \neq i' \Rightarrow \mu_i \neq \mu_i'$, *such that, for the indeterminate* U,

- *the minimal polynomials* $P_{r_1}(U)$ *and* $P_{r_d}(U^d)$ *are respectively given by*

$$
\begin{aligned}
&P_{r_1}(U) = \prod_{i=1}^{r_1} (U - \mu_i), \\
&P_{r_d}(U^d) = \prod_{i=1}^{r_d} (U^d - \mu_i^d), \quad r_d \leq r_1, \\
&P_{r_1}(U) \mid P_{r_d}(U^d).
\end{aligned}
$$

- *The coefficients of $P_{r_d}(U^d)$ are explicitly computable by*

  $$P_{r_d}(U^d) =$$
  $$U^{dr_d} - S_1(d) \times U^{d(r_d-1)} + S_2(d) \times U^{d(r_d-2)} + \dots + (-1)^{r_d-1} S_{r_d-1}(d) \times U^d + (-1)^{r_d} S_{r_d}(d),$$
  $$S_0(d) = 1,$$
  $$S_1(d) = \sum_{i=1,\dots,r_d} \mu_i^d,$$
  $$S_2(d) = \sum_{1 \le i_1 < i_2 \le r_d} \mu_{i_1}^d \mu_{i_2}^d,$$
  $$\vdots$$
  $$S_{r_d}(d) = \mu_1^d \mu_2^d \dots \mu_{r_d}^d.$$

- *Then the ideal*

  $$\prod_{i=0}^{r_d} \sigma^{di}(\mathbf{b})^{(-1)^{r_d-i} \times S_{r_d-i}(d)} = \mathbf{b}^{P_{r_d}(\sigma^d)} \tag{4}$$

  is a principal ideal.

Remark: For other annihilation methods of $Cl(\mathbb{Q}(\zeta)/\mathbb{Q})$ more involved, see for instance Kummer, in Ribenboim [6] p 119, (2C) and (2D) and Stickelberger in Washington [9] p 94 and 332.

3.3 On the structure of the p-class group of subfields of $\mathbb{Q}(\zeta)$

In this subsection we get several results on the structure of the p-class group of $\mathbb{Q}(\zeta)$ and on class number h of $\mathbb{Q}(\zeta)$:

- A formulation, with our notations, of a Ribet's result on irregularity index.
- Let $d, g \in \mathbb{N}$ coprime with $d \times g = p - 1$. For groups generated by the action of Galois groups G and of subgroups G_d, G_g of G on ideals $\mathbf{b}$ of $\mathbb{Q}(\zeta)$, an inequality between degrees r_1, r_d, r_g in the indeterminate X of minimal polynomials $P_{r_1}(X), P_{r_d}(X), P_{r_g}(X) \in \mathbf{F}_p[X]$, with $P_{r_1}(\sigma), P_{r_d}(\sigma^d), P_{r_g}(\sigma^g)$ annihilating ideal class of $\mathbf{b}$.
- Some π-adic congruences connected to structure of p-class group C_p of $\mathbb{Q}(\zeta)$.

3.3.1 Some definitions and notations

- Recall that:
  - r_p is the p-rank of the class group of $\mathbb{Q}(\zeta)$.
  - C_p is the subgroup of exponent p of the p-class group of $\mathbb{Q}(\zeta)$.
- The $\mathbb{Q}$-isomorphism σ of $\mathbb{Q}(\zeta)$ generates $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$, Galois group of the field $\mathbb{Q}(\zeta)$. For $d \mid p-1$, let G_d be the subgroup of d powers σ^{di} of elements σ^i of G. This group is of order $\frac{p-1}{d}$.
- Suppose that $r_p > 0$. There exists an ideal class with representants $\mathbf{b} \subset \mathbb{Z}[\zeta]$, with $\mathbf{b}^p \simeq \mathbb{Z}[\zeta], \quad \mathbf{b} \not\simeq \mathbb{Z}[\zeta]$, which verifies, in term of representations, for some ideals $\mathbf{b}_i$ of $\mathbb{Z}[\zeta], \quad i = 1, \dots, r_p$,

$$
\begin{aligned}
&\mathbf{b} \simeq \prod_{i=1}^{r_p} \mathbf{b}_i,\\
&\mathbf{b}_i^p \simeq \mathbb{Z}[\zeta], \quad \mathbf{b}_i \not\simeq \mathbb{Z}[\zeta], \quad i = 1, \dots, r_p,\\
(5) \qquad &\sigma(\mathbf{b}_i) \simeq \mathbf{b}_i^{\mu_i}, \quad \mu_i \in \mathbf{F}_p, \quad \mathbf{b}_i + \pi = \mathbb{Z}[\zeta], \quad i = 1, \dots, r_p,\\
&C_p = \oplus_{i=1}^{r_p} < Cl(\mathbf{b}_i) >,\\
&P_{r_1}(U) = \prod_{i=1}^{r_1} (U - \mu_i), \quad \mathbf{b}^{P_{r_1}(\sigma)} \simeq \mathbb{Z}[\zeta], \quad 1 \leq r_1 \leq r_p,
\end{aligned}
$$

  where $P_{r_1}(U)$ is the minimal polynomial in the indeterminate U for the action of G on the ideal $\mathbf{b}$, such that $P_{r_1}(\sigma) \in \mathbf{F}_p[G]$ annihilates the ideal class of $\mathbf{b}$, see theorem 3.3 p 13. Recall that it is possible to encounter the case $\mu_i = \mu_j$ in the set $\{\mu_1, \dots, \mu_{r_p}\}$; by opposite if $U - \mu_i$ and $U - \mu_j$ divide the minimal polynomial $P_{r_1}(U)$ then $\mu_i \neq \mu_j$. Therefore r_1 is the degree of the minimal polynomial $P_{r_1}(U)$.
- With a certain indexing assumed in the sequel, the ideals classes $Cl(\mathbf{b}_i) \in C_p^-$ for $i = 1, \dots, r_p^-$, and ideal classes $Cl(\mathbf{b}_i) \in C_p^+$ for $i = r_p^- + 1, \dots, r_p$.
  - The ideal $\mathbf{b}$ verifies $\mathbf{b} \simeq \mathbf{b}^- \times \mathbf{b}^+$ where $\mathbf{b}^-$ and $\mathbf{b}^+$ are two ideals of $\mathbb{Q}(\zeta)$ with $Cl(\mathbf{b}^-) \in C_p^-$ and $Cl(\mathbf{b}^+) \in C_p^+$.
  - With this notation, the minimal polynomial $P_{r_1}(U)$ factorize in a factor corresponding to C_p^- and a factor corresponding to C_p^+, with:

$$
(6) \qquad P_{r_1}(U) = P_{r_1^-}(U) \times P_{r_1^+}(U), \quad r_1 = r_1^- + r_1^+.
$$

– $P_{r_1^-}(U)$ is the minimal polynomial with $P_{r_1^-}(\sigma) \in \mathbf{F}_p[G]$ annihilating the class of ideal $\mathbf{b}^- \in C_p^-$.
– $P_{r_1^+}(U)$ is the minimal polynomial with $P_{r_1^+}(\sigma) \in \mathbf{F}_p[G]$ annihilating the class of ideal $\mathbf{b}^+ \in C_p^+$.

- Let us denote $M_{r_1} = \{\mu_i \quad | \quad i = 1, \dots, r_1\}$.
- Let $d \in \mathbb{N}, \quad d \mid p-1, \quad 2 \le d \le \frac{p-1}{2}$. Let K_d be the field $\mathbb{Q} \subset K_d \subset \mathbb{Q}(\zeta), \quad [K_d : \mathbb{Q}] = d$.
- Let $P_{r_d}(V)$ be the minimal polynomial in the indeterminate V of the action of the group G_d on the ideal class group $< \mathbf{b} >$ of order p, such that $P_{r_d}(\sigma^d) \in \mathbf{F}_p[G_d]$ annihilates ideal class of $\mathbf{b}$. Let r_d be the degree of $P_{r_d}(V)$.

3.3.2 On the irregularity index

Recall that r_p is the p-rank of the group C_p. The irregularity index is the number

$$i_p = Card\{B_{p-1-2m} \mid B_{p-1-2m} \equiv 0 \bmod p, \quad 1 \le m \le \frac{p-3}{2}\},$$

where B_{p-1-2m} are even Bernoulli Numbers. The next theorem connects irregularity index and degree r_1^- of minimal polynomial $P_{r_1^-}(U)$ defined in relations (5) p. 15 and 6 p. 15.

Theorem 3.4. **** With meaning of degree r_1^- of minimal polynomial $P_{r_1^-}(U)$ defined in relation (6) p. 15, then the irregularity index is equal to the degree r_1^- and verifies :*

$$r_p^- - r_p^+ \le i_p = r_1^- \le r_p^-. \tag{7}$$

Proof. Let us consider in relation (5) the set of ideals $\{\mathbf{b}_i \mid i = 1, \dots, r_p\}$. The result of Ribet using theory of modular forms [7] mentionned in Ribenboim [6] (8C) p 190 can be formulated, with our notations,

$$B_{p-1-2m} \equiv 0 \bmod p \Leftrightarrow \exists i, \quad 1 \le i \le r_p, \quad \mathbf{b}_i^{\sigma - u_{2m+1}} \simeq \mathbb{Z}[\zeta]. \tag{8}$$

There exists at least one such i, but it is possible for $i \ne i'$ that $\mathbf{b}_i^{\sigma - u_{2m+1}} \simeq \mathbf{b}_{i'}^{\sigma - u_{2m+1}} \simeq \mathbb{Z}[\zeta]$.

- The relation (8) p. 16 implies that $i_p = r_1^-$.
- The inequality (7) p. 16 is an immediate consequence of independant forward structure theorem 3.15 p. 27.

□

3.3.3 Inequalities involving degrees r_1, r_d, r_g of minimal polynomials $P_{r_1}(V), P_{r_d}(V), P_{r_g}(V)$ annihilating ideal b.

In this subsection, we always assume that $\mathbf{b}$ is defined by relation (5) p. 15.

Let p be an odd prime. Let $d, g \in \mathbb{N}$, with $gcd(d,g) = 1$ and $d \times g = p-1$. Recall that r_1, r_d and r_g are the degrees of the minimal polynomials $P_{r_1}(V), P_{r_d}(V), P_{r_g}(V)$ of the indeterminate V with $\mathbf{b}^{P_{r_1}(\sigma)} \simeq \mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbf{b}^{P_{r_g}(\sigma^g)} \simeq \mathbb{Z}[\zeta]$. The next theorem is a relation between the three degree r_1, r_d and r_g.

Theorem 3.5. **** Let $d, g \in \mathbb{N}, \quad gcd(d,g) = 1, \quad d \times g = p-1$. Suppose that $r_d \geq 1$ and $r_g \geq 1$. Then*

$$r_d \times r_g \geq r_1. \tag{9}$$

and if $r_d = 1$ then $r_g = r_1$.

Proof.

- Let us consider the minimal polynomials $P_{r_d}(U^d) = \prod_{i=1}^{r_d}(U^d - \mu_i^d)$ and $P_{r_g}(U^g) = \prod_{i=1}^{r_g}(U^g - \nu_j^g)$ of the indeterminate U with $\mathbf{b}^{P_{r_d}(\sigma^d)} \simeq \mathbb{Z}[\zeta]$ and $\mathbf{b}^{P_{r_g}(\sigma^g)} \simeq \mathbb{Z}[\zeta]$.
- From lemma 3.2 p.11, we have seen that $P_{r_1}(U) \mid P_{r_d}(U^d)$ and that similarly $P_{r_1}(U) \mid P_{r_g}(U^g)$, thus $P_{r_1}(U) \mid gcd(P_{r_d}(U^d), P_{r_g}(U^g))$.
- Let $M_{r_1} = \{\mu_i \quad | \quad i = 1, \dots, r_1\}$. Let us define the sets

  $$C_1(\mu_i) = \{\mu_i \times \alpha_j \quad | \quad \alpha_j^d = 1, \quad j = 1, \dots, d\} \cap M_{r_1}, \quad i = 1, \dots, r_d.$$

  Let us define in the same way the sets

  $$C_2(\nu_i) = \{\nu_i \times \beta_j \quad | \quad \beta_j^g = 1, \quad j = 1, \dots, g\} \cap M_{r_1}, \quad i = 1, \dots, r_g.$$

- We have proved in lemma 3.2 p.11 that $P_{r_1}(U) \mid P_{r_d}(U^d)$. Therefore the sets $C_1(\mu_i), \quad i = 1, \dots, r_d$, are a partition of M_{r_1} and $r_1 = \sum_{i=1}^{r_d} Card(C_1(\mu_i))$.
- In the same way $P_{r_1}(U) \mid P_{r_g}(U^g)$. Therefore the sets $C_2(\nu_i), \quad i = 1, \dots, r_g$, are a partition of M_{r_1} and $r_1 = \sum_{i=1}^{r_g} Card(C_2(\nu_i))$.
- There exists at least one $i \in \mathbb{N}, \quad 1 \leq i \leq r_d$, such that $Card(C_1(\mu_i)) \geq \frac{r_1}{r_d}$. For this i, let $\nu_1 = \mu_i \times \alpha_1, \quad \alpha_1^d = 1, \quad \nu_1 \in M_{r_1}$ and, in the same way, let $\nu_2 = \mu_i \times \alpha_2, \quad \alpha_2^d = 1, \quad \nu_2 \in M_{r_1}, \quad \nu_2 \neq \nu_1$. We have $\nu_1^g \neq \nu_2^g$: if not we should simultaneously have $\alpha_1^d = \alpha_2^d$ and $\alpha_1^g = \alpha_2^g$, which should imply, from $gcd(d,g) = 1$, that $\alpha_1 = \alpha_2$, contradicting $\nu_1 \neq \nu_2$ and therefore we get $C_2(\nu_1) \neq C_2(\nu_2)$.

- Therefore, extending the same reasoning to all elements of $C_1(\mu_i)$, we get $\frac{r_1}{r_d} \leq Card(C_1(\mu_i)) \leq r_g$, which leads to the result.

- If $r_d = 1$ then $r_g \geq r_1$ and in an other part $r_g \leq r_1$ and so $r_g = r_1$.

$\square$

Remarks:

- As an example, consider an odd prime p verifying $p \not\equiv 1 \mod 4$. Suppose also that $h^+ \not\equiv 0 \mod p$. Then $P_{r_{(p-1)/2}}(\sigma) = \sigma^{(p-1)/2} + 1 = U + 1$ for the indeterminate $U = \sigma^{(p-1)/2}$. Therefore $r_{(p-1)/2} = 1$ and thus $r_2 = r_1$.

- Observe that $1 \leq r_d < r_1$ implies that $r_g > 1$.

3.3.4 On Stickelberger's ideal in field $\mathbb{Q}(\zeta)$

In this subsection, we give a result resting on the annihilation of class group of $\mathbb{Q}(\zeta)$ by Stickelberger's ideal.

- Let us denote $\mathbf{a} \simeq \mathbf{c}$ when the two ideals $\mathbf{a}$ and $\mathbf{c}$ of $\mathbb{Q}(\zeta)$ are in the same ideal class.

- Let $G = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$.

- Let $\tau_a : \zeta \to \zeta^a, \quad a = 1, \dots, p-1$, be the $p-1$ $\mathbb{Q}$-isomorphisms of the field $\mathbb{Q}(\zeta)/\mathbb{Q}$.

- Recall that u is a primitive root $\mod p$, and that $\sigma : \zeta \to \zeta^u$ is a $\mathbb{Q}$-isomorphism of the field $\mathbb{Q}(\zeta)$ which generates G. Recall that, for $i \in \mathbb{N}$, then we denote u_i for $u^i \mod p$ and $1 \leq u_i \leq p-1$.

- Let $\mathbf{b}$ be the not principal ideal defined in relation (5) p.15. Let $P_{r_1}(\sigma) \in \mathbf{F}_p[G]$ be the polynomial of minimal degree such that $P_{r_1}(\sigma)$ annihilates $\mathbf{b}$, so such that $\mathbf{b}^{P_{r_1}(\sigma)}$ is principal ideal, see lemma 3.1 p.10, and so

$$P_{r_1}(\sigma) = \prod_{i=1}^{r_1} (\sigma - \mu_i), \quad \mu_i \in \mathbf{F}_p, \quad i \neq i' \Rightarrow \mu_i \neq \mu'_i.$$

In the next result we shall explicitly use the annihilation of class group of $\mathbb{Q}(\zeta)$ by the Stickelberger's ideal.

Lemma 3.6. *Let $P_{r_1}(U) = \prod_{i=1}^{r_1}(U - \mu_i)$ be the polynomial of the indeterminate U, of minimal degree, such that $\mathbf{b}^{P_{r_1}(\sigma)}$ is principal. Then $\mu_i \neq u, \quad i = 1, \dots, r_1$.*

Proof.

- Let $i \in \mathbb{N}, \quad 1 \leq i \leq r_1$. From relation (5) p.15, there exists ideals $\mathbf{b}_i \in \mathbb{Z}[\zeta], \quad i = 1, \ldots, r_p$, not principal and such that $\mathbf{b} = \prod_{i=1}^{r_p} \mathbf{b}_i$, with $\mathbf{b}_i^{\sigma-\mu_i}$ principal.

- Suppose that $\mu_i = u$, and search for a contradiction: Let us consider $\theta = \sum_{a=1}^{p-1} \frac{a}{p} \times \tau_a^{-1} \in \mathbb{Q}[G]$. Then $p\theta \in \mathbb{Z}[G]$ and the ideal $\mathbf{b}^{p\theta}$ is principal from Stickelberger's theorem, see for instance Washington [9], theorem 6.10 p 94.

- We can set $a = u^m, \quad a = 1, \ldots, p-1$, and m going through all the set $\{0, 1, \ldots, p-2\}$, because u is a primitive root $\mod p$. Then $\tau_a : \zeta \rightarrow \zeta^a$ and so $\tau_a^{-1} : \zeta \rightarrow \zeta^{(a^{-1})} = \zeta^{((u^m)^{-1})} = \zeta^{(u^{-m})} = \zeta^{(u^{p-1-m})} = \sigma^{p-1-m} = \sigma^{-m}$.

- Therefore, $p\theta = \sum_{m=0}^{p-2} u^m \sigma^{-m}$. The element $\sigma - \mu_i = \sigma - u$ annihilates the class of $\mathbf{b}_i$ and also the element $u \times \sigma^{-1} - 1$ annihilates the class of $\mathbf{b}_i$. Therefore $u^m \sigma^{-m} - 1, \quad m = 0, \ldots, p-2$, annihilates the class of $\mathbf{b}_i$ and finally $p-1$ annihilates the class of $\mathbf{b}_i$, so $\mathbf{b}_i^{p-1}$ is principal, but $\mathbf{b}_i^p$ is also principal, and finally $\mathbf{b}_i$ is principal which contradicts our hypothesis and achieves the proof.

□

3.4 π-adic congruences connected to p-class group C_p

In a first subsection, we examine the case of relative p-class group C_p^-. In a second subsection, we examine the case of p-class group C_p^+. In last subsection, we summarize our results to all p-class group C_p. These important congruences (subjective) characterize structure of p-class group.

3.4.1 π-adic congruences connected to relative p-class group C_p^-

In this subsection , we shall describe some π-adic congruences connected to p-relative class group C_p^-.

Some definitions and a preliminary result

- Let C_p be the subgroup of exponent p of the p-class group of $\mathbb{Q}(\zeta)$.

- Let r_p be the p-rank of C_p, let r_p^+ be the p-rank of C_p^+ and r_p^- be the relative p-rank of C_p^-. Let us recall the structure of the ideal $\mathbf{B}$ already defined in

relation (5) p.15:

$$(10)\qquad \begin{aligned}
&\mathbf{B}=\mathbf{b}_1\times\cdots\times\mathbf{b}_{r_p^-}\times\mathbf{b}_{r_p^-+1}\times\cdots\times\mathbf{b}_{r_p},\\
&C_p=\oplus_{i=1}^{r_p}<Cl(\mathbf{b}_i)>,\\
&\mathbf{b}_i^p\simeq\mathbb{Z}[\zeta],\quad \mathbf{b}_i\not\simeq\mathbb{Z}[\zeta],\quad i=1,\dots,r_p,\\
&\sigma(\mathbf{b}_i)\simeq\mathbf{b}_i^{\mu_i},\quad \mu_i\in\mathbf{F}_p^*,\quad i=1,\dots,r_p,\\
&Cl(\mathbf{b}_i)\in C_p^-,\quad i=1,\dots,r_p^-,\\
&Cl(\mathbf{b}_i)\in C_p^+,\quad i=r_p^-+1,\dots,r_p,\\
&\mathbf{B}^{P_{r_1}(\sigma)}\simeq\mathbb{Z}[\zeta],\\
&(\frac{\mathbf{B}}{\overline{\mathbf{B}}})^{P_{r_1^-}(\sigma)}\simeq\mathbb{Z}[\zeta].
\end{aligned}$$

(Observe that we replace here notation $\mathbf{b}$ by $\mathbf{B}$ to avoid conflict of notation in the sequel.) In the sequel, we are using also the natural integers m_i, with $0\le m_i\le\frac{p-3}{2}$, defined by $\mu_i=u_{2m_i+1}=u^{2m_i+1}$ mod p.

- Recall that it is possible to have $\mu_i=\mu_j=\mu$: observe that, in that case, the decomposition $<Cl(\mathbf{b}_i)>\oplus<Cl(\mathbf{b}_j)>$ is not unique. We can have

$$\begin{aligned}
&<Cl(\mathbf{b}_i)>\oplus<Cl(\mathbf{b}_j)>=<Cl(\mathbf{b}'_i)>\oplus<Cl(\mathbf{b}'_j)>,\\
&\sigma(\mathbf{b}_i)\simeq\mathbf{b}_i^{\mu},\quad\sigma(\mathbf{b}_j)\simeq\mathbf{b}_j^{\mu},\quad\sigma(\mathbf{b}'_i)\simeq(\mathbf{b}'_i)^{\mu},\quad\sigma(\mathbf{b}'_j)\simeq(\mathbf{b}'_j)^{\mu},\\
&<Cl(\mathbf{b}_i)>\notin\{<Cl(\mathbf{b}_j)>,\quad<Cl(\mathbf{b}'_i)>,\quad<Cl(\mathbf{b}'_j)>\}.
\end{aligned}$$

- Recall that $P_{r_1}(\sigma)\in\mathbf{F}_p[G]$ is the minimal polynomial such that $\mathbf{b}^{P_{r_1}(\sigma)}\simeq\mathbb{Z}[\zeta]$ with $r_1\le r_p$.

- Recall that $P_{r_1^-}(\sigma)\in\mathbf{F}_p[G]$ is the minimal polynomial such that $(\frac{\mathbf{b}}{\overline{\mathbf{b}}})^{P_{r_1}(\sigma)}\simeq\mathbb{Z}[\zeta]$ with $r_1^-\le r_p^-$.

- We say that the algebraic number $C\in\mathbb{Q}(\zeta)$ is singular if $C\mathbb{Z}[\zeta]=\mathbf{c}^p$ for some ideal $\mathbf{c}$ of $\mathbb{Q}(\zeta)$. We say that C is singular primary if C is singular and $C\equiv c^p$ mod π^p, $\quad c\in\mathbb{Z},\quad c\not\equiv 0$ mod p.

At fisrt, a general lemma dealing with congruences on p-powers of algebraic numbers of $\mathbb{Q}(\zeta)$.

Lemma 3.7. *Let $\alpha,\beta\in\mathbb{Z}[\zeta]$ with $\alpha\not\equiv 0\mod\pi$ and $\alpha\equiv\beta$ mod π. Then $\alpha^p\equiv\beta^p$ mod π^{p+1}.*

Proof. Let $\lambda = (\zeta - 1)$. Then $\alpha - \beta \equiv 0 \bmod \pi$ implies that $\alpha - \zeta^k\beta \equiv 0 \bmod \pi$ for $k = 0, 1, \dots, p-1$. Therefore, for all k, $\quad 0 \leq k \leq p-1$, there exists $a_k \in \mathbb{N}$, $\quad 0 \leq a_k \leq p-1$, such that $(\alpha - \zeta^k\beta) \equiv \lambda a_k \bmod \pi^2$. For another value l, $\quad 0 \leq l \leq p-1$, we have, in the same way, $(\alpha - \zeta^l\beta) \equiv \lambda a_l \bmod \pi^2$, hence $(\zeta^k - \zeta^l)\beta \equiv \lambda(a_k - a_l) \bmod \pi^2$. For $k \neq l$ we get $a_k \neq a_l$, because $\pi \| (\zeta^k - \zeta^l)$ and because hypothesis $\alpha \not\equiv 0 \bmod \pi$ implies that $\beta \not\equiv 0 \bmod \pi$. Therefore, there exists one and only one k such that $(\alpha - \zeta^k\beta) \equiv 0 \bmod \pi^2$. Then, we have $\prod_{j=0}^{p-1}(\alpha - \zeta^j\beta) = (\alpha^p - \beta^p) \equiv 0 \bmod \pi^{p+1}$. $\square$

For $i = 1, \dots, r_p^-$, to simplify notations in this lemma, let us note respectively $\mathbf{b}, B, C, \mu = u_{2m+1}$ for $\mathbf{b}_i, B_i, C_i, \mu_i = u_{2m_i+1}$ as defined in the two relations (10) p. 20 and (14) p. 22.

Lemma 3.8. *For $i = 1, \dots, r_p^-$, there exists algebraic integers $B \in \mathbb{Z}[\zeta]$ such that*

$$\begin{aligned}
&B\mathbb{Z}[\zeta] = \mathbf{b}^p,\\
&\sigma(\frac{B}{\overline{B}}) \times (\frac{B}{\overline{B}})^{-\mu} = (\frac{\alpha}{\overline{\alpha}})^p, \quad \alpha \in \mathbb{Q}(\zeta), \quad \alpha\mathbb{Z}[\zeta] + \pi = \mathbb{Z}[\zeta],\\
&\sigma(\frac{B}{\overline{B}}) \equiv (\frac{B}{\overline{B}})^{\mu} \ \mathit{mod}\ \pi^{p+1}.
\end{aligned} \tag{11}$$

Proof.

1. Observe that we can neglect in this proof the values $\mu = u_{2m}$ such that $\sigma - \mu$ annihilates ideal classes $\in C_p^+$, because we consider only quotients $\frac{B}{\overline{B}}$, with ideal classes $Cl(\mathbf{b})$ in C_p^-. The ideal $\mathbf{b}^p$ is principal. So let one $\beta \in \mathbb{Z}[\zeta]$ with $\beta\mathbb{Z}[\zeta] = \mathbf{b}^p$. We have seen in relation (5) p.15 that $\sigma(\mathbf{b}) \simeq \mathbf{b}^\mu$, therefore there exists $\alpha \in \mathbb{Q}(\zeta)$ such that $\frac{\sigma(\mathbf{b})}{\mathbf{b}^\mu} = \alpha\mathbb{Z}[\zeta]$, also $\frac{\sigma(\beta)}{\beta^\mu} = \varepsilon \times \alpha^p$, $\quad \varepsilon \in \mathbb{Z}[\zeta]^*$. Let $B = \delta^{-1} \times \beta$, $\quad \delta \in \mathbb{Z}[\zeta]^*$, for a choice of the unit δ that whe shall explicit in the next lines. We have

$$\sigma(\delta \times B) = \alpha^p \times (\delta \times B)^\mu \times \varepsilon.$$

Therefore

$$\sigma(B) = \alpha^p \times B^\mu \times (\sigma(\delta^{-1}) \times \delta^\mu \times \varepsilon). \tag{12}$$

From Kummer's lemma on units, we can write

$$\begin{aligned}
\delta &= \zeta^{v_1} \times \eta_1, \quad v_1 \in \mathbb{Z}, \quad \eta_1 \in \mathbb{Z}[\zeta + \zeta^{-1}]^*,\\
\varepsilon &= \zeta^{v_2} \times \eta_2, \quad v_2 \in \mathbb{Z}, \quad \eta_2 \in \mathbb{Z}[\zeta + \zeta^{-1}]^*.
\end{aligned}$$

Therefore

$$\sigma(\delta^{-1}) \times \delta^\mu \times \varepsilon = \zeta^{-v_1 u + v_1\mu + v_2} \times \eta, \quad \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^*.$$

From lemma 3.6 p.18, we deduce that $\mu \neq u$, therefore there exists one v_1 with $-v_1 u + v_1\mu + v_2 \equiv 0 \mod p$. Therefore, chosing this value v_1 for the unit δ,

$$\begin{aligned} &\sigma(B) = \alpha^p \times B^\mu \times \eta, \quad \alpha\mathbb{Z}[\zeta] + \pi = \mathbb{Z}[\zeta], \quad \eta \in \mathbb{Z}[\zeta + \zeta^{-1}]^*, \\ &\sigma(\overline{B}) = \overline{\alpha}^p \times \overline{B}^\mu \times \eta. \end{aligned} \tag{13}$$

We have $\alpha \equiv \overline{\alpha} \mod \pi$ and we have proved in lemma 3.7 p.20 that $\alpha^p \equiv \overline{\alpha}^p \mod \pi^{p+1}$, which leads to the result.

□

π-adic congruences connected to relative p-class group C_p^- : For $i = 1, \dots, r_p^-$, to simplify notations in this lemma, let us note respectively $\mathbf{b}, B, C, \mu = u_{2m+1}$ for $\mathbf{b}_i, B_i, C_i, \mu_i = u_{2m_i+1}$ as defined in the two relations (10) p. 20 and (14) p. 22.

Lemma 3.9. *For each $i = 1, \dots, r_p^-$, there exists singular algebraic integers $B \in \mathbb{Z}[\zeta]$, such that*

$$\begin{aligned} &\mu = u_{2m+1}, \quad m \in \mathbb{N}, \quad 1 \leq m \leq \frac{p-3}{2}, \\ &B\mathbb{Z}[\zeta] = \mathbf{b}^p, \\ &C = \frac{B}{\overline{B}} \equiv 1 \ mod\ \pi^{2m+1}. \end{aligned} \tag{14}$$

Then, either C is singular not primary with $\pi^{2m+1} \parallel C - 1$ or C is singular primary with $\pi^p \mid C - 1$.

Proof.

- The definition of C implies that $C \equiv 1 \mod \pi$, and so that $\sigma(C) \equiv 1 \mod \pi$. There exists a natural integer ν such that $\pi^\nu \parallel C - 1$, therefore we can write

$$\begin{aligned} &C \equiv 1 + c_0\lambda^\nu \mod \lambda^{\nu+1}, \\ &c_0 \in \mathbb{Z}, \quad c_0 \not\equiv 0 \mod p. \end{aligned} \tag{15}$$

  We have to prove that $\nu < p$ implies that $\nu = 2m + 1$ for the integer $m < p - 1$ verifying $\mu = u_{2m+1}$.

- From lemma 3.8 p.21, it follows that $\sigma(C) = C^\mu \times \alpha^p$, with some $\alpha \in \mathbb{Q}(\zeta)$, and so that $1 + c_0\sigma(\lambda)^\nu \equiv (1 + \mu c_0\lambda^\nu) \times \alpha^p \mod \pi^{\nu+1}$. This congruence implies that $\alpha \equiv 1 \mod \pi$ and then, from lemma 3.7, $\alpha^p \equiv 1 \mod \pi^{p+1}$. Then $1 + c_0\sigma(\lambda)^\nu \equiv 1 + \mu c_0\lambda^\nu \mod \lambda^{\nu+1}$, and so $\sigma(\lambda^\nu) \equiv \mu\lambda^\nu \mod \pi^{\nu+1}$. This

implies that $\sigma(\zeta-1)^\nu \equiv \mu\lambda^\nu \mod \pi^{\nu+1}$, so that $(\zeta^u-1)^\nu \equiv \mu\lambda^\nu \mod \pi^{\nu+1}$, so that $((\lambda+1)^u-1)^\nu \equiv \mu\lambda^\nu \mod \pi^{\nu+1}$ and finally $u^\nu\lambda^\nu \equiv \mu\lambda^\nu \mod \pi^{\nu+1}$, with simplification $u^\nu - \mu \equiv 0 \mod \pi$. Therefore, we have proved that $\nu = 2m+1$ or that, when $\pi^p \not| C-1$, then $\pi^{2m+1} \parallel C-1$.

□

Remarks:

1. In considering $\mathbf{b}^{p-1}$ in place of $\mathbf{b}$, we consider B^{p-1} and C^{p-1} in place of B and C, such that we can always assume without loss of generality that $B \equiv C \equiv 1 \mod \pi$. We suppose implicitely this normalization in the sequel.
2. In relation (15) we can suppose without loss of generality that $c_0 = 1$ because we can consider $\mathbf{b}^n$ with $1 \leq n \leq p-1$ in place of $\mathbf{b}$ with $n \times c_0 \equiv 1 \mod p$. We suppose implicitely this normalization in the sequel.

As previously, for $i = 1, \dots, r_p$, to simplify notations in this lemma, let us note respectively $\mathbf{b}, B, C, \mu = u_{2m+1}$ for $\mathbf{b}_i, B_i, C_i, \mu_i = u_{2m_i+1}$ as defined in the two relations (10) p. 20 and (14) p. 22. In the following lemma, we connect π-adic congruences on $C-1$ with $C = \frac{B}{\overline{B}}$ to some π-adic congruences on algebraic integer B.

Theorem 3.10. *****

1. *If the singular number B is not primary, there exists a primary unit $\eta \in \mathbb{Z}[\zeta+\zeta^{-1}] - \{1,-1\}$ and a singular not primary number $B' = \frac{B^2}{\eta}$, such that*

$$\begin{aligned} &\sigma(B') = B'^\mu \times \alpha^p, \quad \alpha \in \mathbb{Q}(\zeta), \\ &B'\mathbb{Z}[\zeta] = \mathbf{b}^{2p}, \quad B' \in \mathbb{Z}[\zeta], \\ &\pi^{2m+1} \parallel (B')^{p-1} - 1. \end{aligned} \tag{16}$$

2. *If the singular number B is primary then*

$$\begin{aligned} &\sigma(B) = B^\mu \times \alpha^p, \quad \alpha \in \mathbb{Q}(\zeta), \\ &B\mathbb{Z}[\zeta] = \mathbf{b}^p, \\ &\pi^{p-1} \mid B-1. \end{aligned} \tag{17}$$

Proof. 1. We have $C\mathbb{Z}[\zeta] = \mathbf{b}^p$ where the ideal $\mathbf{b}$ verifies $\sigma(\mathbf{b}) \simeq \mathbf{b}^\mu$ and $Cl(\mathbf{b}) \in C_p^-$. From relation (13) p. 22 and from $Cl(\mathbf{b}) \in C_p^-$, we can choose B such

that

$C=\frac{B}{\overline{B}}, \quad B\in\mathbb{Z}[\zeta],$

$B\overline{B}=\eta\times\gamma^p, \quad \eta\in\mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad \gamma\in\mathbb{Q}(\zeta), \quad v_\pi(\gamma)=0,$

$\sigma(B)=B^\mu\times\alpha^p\times\varepsilon, \quad \mu=u_{2m+1}, \quad \alpha\in\mathbb{Q}(\zeta), \quad v_\pi(\alpha)=0, \quad \varepsilon\in\mathbb{Z}[\zeta+\zeta^{-1}]^*.$

We derive that

$$\sigma(B\overline{B})=\sigma(\eta)\times\sigma(\gamma^p)$$
$$\sigma(B\overline{B})=(B\overline{B})^\mu\times(\alpha\overline{\alpha})^p\times\varepsilon^2=\eta^\mu\gamma^{p\mu}\times(\alpha\overline{\alpha})^p\times\varepsilon^2,$$

and so

$$\sigma(\eta)=\eta^\mu\times\varepsilon^2\times\varepsilon_1^p, \quad \varepsilon_1\in\mathbb{Z}[\zeta+\zeta^{-1}]^*.$$

We have seen that

$$\sigma(B^2)=B^{2\mu}\times\alpha^{2p}\times\varepsilon^2,$$

and so

$$\sigma(B^2)=B^{2\mu}\times\alpha^{2p}\times(\sigma(\eta)\eta^{-\mu}\varepsilon_1^{-p})$$

which leads to

$$\sigma(\frac{B^2}{\eta})=(\frac{B^2}{\eta})^\mu\times\alpha_2^p, \quad \alpha_2^p=\alpha^{2p}\times\varepsilon_1^{-p}, \quad \alpha_2\in\mathbb{Q}(\zeta), \quad v_\pi(\alpha_2)=0.$$

Let us note $B'=\frac{B^2}{\eta}, \quad B'\in\mathbb{Z}(\zeta), \quad v_\pi(B')=0$. We get

$$\sigma(B')=(B')^\mu\times\alpha_2^p. \tag{18}$$

This relation (18) is similar to hypothesis used to prove lemma 3.9 p. 22. This leads in the same way to $B'\equiv d^p \bmod \pi^{2m+1}, \quad d\in\mathbb{Z}, \quad d\not\equiv 0 \bmod p$. Therefore $(B')^{p-1}\equiv 1 \bmod \pi^{2m+1}$, which achieves the proof of the first part.

2. We have

$$\begin{aligned}\sigma(B)&=B^\mu\times\alpha^p\times\eta, \quad \eta\in\mathbb{Z}[\zeta+\zeta^{-1}]^*\\ \sigma(\overline{B})&=\overline{B}^\mu\times\overline{\alpha}^p\times\eta.\end{aligned} \tag{19}$$

From **simultaneous** application of a Furtwangler theorem, see Ribenboim [6] (6C) p. 182 and of a Hecke theorem on class field theory, see Ribenboim [6] (6D) p. 182, it results that

$$B\times\overline{B}=\beta^p \tag{20}$$

where $\beta\in\mathbb{Z}[\zeta]-\mathbb{Z}[\zeta+\zeta^{-1}]^*$. From these two relations, it follows that $\eta\in(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$, which achieves the proof of the second part.

□

On structure of p-class group C_p^-

In this paragraph, the indexing of singular primary and of singular not primary C_i with usual previously defined meaning of index $i = 1, \dots, r_p^+, r_p^+ + 1, \dots, r_p^-$, is used to describe the structure of relative p-class group C_p^-: we shall show that, with a certain ordering of index i, then C_i are singular primary for $i = 1, \dots, r_p^+$ and C_i are singular not primary for $i = r_p^+ + 1, \dots, r_p^-$.

Theorem 3.11. **** Let $\mathbf{C} = C_1^{\alpha_1} \times \dots \times C_i^{\alpha_i} \times \dots \times C_n^{\alpha_n}$ with $\alpha_i \in \mathbf{F}_p^*$, $\quad 1 \leq n \leq r_p^-$ and with $\mu_i = u_{2m_i+1}$ pairwise different for $i = 1, \dots, n$. Then C is singular primary if and only if all the C_i, $\quad i = 1, \dots, n$, are all singular primary.*

Proof.

- If C_i, $\quad i = 1, \dots, n$, are all singular primary, then C is clearly singular primary.
- Suppose that C_i, $\quad i = 1, \dots, l$, are not singular primary and that C_i, $\quad i = l + 1, \dots, n$, are singular primary. Then, from lemma 3.9 p.22 and remark following it, $\pi^{2m_i+1} \| \ C_i - 1$, $\quad i = 1, \dots, l$, where we suppose, without loss of generality, that $1 < 2m_1 + 1 < \dots < 2m_l + 1$. Then $\pi^{2m_1+1} \parallel C - 1$ and so C is not singular primary, contradiction which achieves the proof.

□

Lemma 3.12. *Let C of relation (14) p. 22. If C is not singular primary, then*

$$C \equiv 1 + V(\mu) \ mod \ \pi^{p-1}, \quad \mu = u_{2m+1} \quad V(\mu) \in \mathbb{Z}[\zeta],$$

where $V(\mu)$ mod p depends only on μ with $\pi^{2m+1} \| \ V(\mu)$.

Proof. The congruence $\sigma(C) \equiv C^{\mu} \bmod \pi^{p+1}$ and the normalization $C \equiv 1 + \lambda^{2m+1} \bmod \pi^{2m+2}$ explained in remark following lemma 3.9 p. 22 implies the result. □

Theorem 3.13. **** Let C_1, C_2 singular not primary defined with relation (14) p. 22. If $\mu_1 = \mu_2$ then $C_1 \times C_2^{-1}$ is singular primary.*

Proof. Let $\mu_1 = \mu_2 = \mu = u_{2m+1}$. Therefore $\sigma(C_1) \equiv C_1^{\mu} \bmod \pi^{p+1}$ and $\sigma(C_2) \equiv C_2^{\mu} \bmod \pi^{p+1}$. From previous lemma 3.12 p. 25 we get

$$\begin{aligned} &C_1 = 1 + V(\mu) + pW_1, \quad W_1 \in \mathbb{Q}(\zeta), \quad v_\pi(V(\mu)) \geq 2m + 1, \quad v_\pi(W_1) \geq 0, \\ &C_2 = 1 + V(\mu) + pW_2, \quad W_2 \in \mathbb{Q}(\zeta), \quad v_\pi(V(\mu)) \geq 2m + 1, \quad v_\pi(W_2) \geq 0, \\ &\pi^{2m+1} \parallel V(\mu), \end{aligned}$$

Elsewhere, C_1, C_2 verify

$$\sigma(C_1) \equiv C_1^{\mu} \bmod \pi^{p+1},$$
$$\sigma(C_2) \equiv C_2^{\mu} \bmod \pi^{p+1},$$

which leads to

$$1 + \sigma(V(\mu)) + p\sigma(W_1) \equiv 1 + A(\mu) + p\mu W_1 \bmod \pi^{p+1},$$
$$1 + \sigma(V(\mu)) + p\sigma(W_2) \equiv 1 + A(\mu) + p\mu W_2 \bmod \pi^{p+1},$$

where $A(\mu) \in \mathbb{Q}(\zeta), \quad v_\pi(A(\mu) \geq 0$ depends only on μ. By difference, we get

$$p(\sigma(W_1 - W_2)) \equiv p\mu(W_1 - W_2) \bmod \pi^{p+1},$$

which implies that

$$\sigma(W_1 - W_2) \equiv \mu(W_1 - W_2) \bmod \pi^2.$$

Let $W_1 - W_2 = a\lambda + b, \quad a, b \in \mathbb{Z}, \quad \lambda = \zeta - 1$. The previous relation implies that $b(1-\mu) \equiv 0 \bmod p$ and so that $a\sigma(\lambda) + b \equiv \mu a\lambda + \mu b \bmod \pi^2$, and so that $b \equiv 0 \bmod p$, because $\mu \neq 1$. Thus $W_1 - W_2 \equiv 0 \bmod \pi$ and finally $C_1 \equiv C_2 \bmod \pi^p$ and also $C_1 C_2^{-1} \equiv 1 \bmod \pi^p$ and $C_1 C_2^{-1}$ is singular primary. □

Corollary 3.14. *Let $C_1, \dots, C_\nu, \quad 1 \leq \nu \leq r_p^-$, singular not primary, defined by relation (14) p. 22.*

1. *If $\mu_1 = \dots = \mu_\nu = \mu$ then $C_1' = C_1 \times C_\nu^{-1}, \dots, C_{\nu-1}' = C_{\nu-1} \times C_\nu^{-1}$ are singular primary.*

2. *In term of ideals, it implies that*

$$\oplus_{i=1}^{\nu} < Cl(\mathbf{b}_i) >= \oplus_{i=1}^{\nu-1} < Cl(\mathbf{b}_i \mathbf{b}_\nu^{-1}) > \oplus < Cl(\mathbf{b}_\nu) >,$$

where $\sigma(\mathbf{b}_i \mathbf{b}_\nu^{-1}) \simeq (\mathbf{b}_i \mathbf{b}_\nu^{-1})^{\mu}$

Proof.

1. Immediate consequence of theorem 3.13 p. 25.

2. $\oplus_{i=1}^{\nu} < Cl(\mathbf{b}_i) >$ is a p-group of rank ν. $\oplus_{i=1}^{\nu-1} < Cl(\mathbf{b}_i \mathbf{b}_\nu^{-1}) >$ is a p-group of rank $\nu - 1$. $< Cl(\mathbf{b}_\nu) >$ is a p-group of rank 1.

□

Remark: It follows that, when $\mu_1 = \cdots = \mu_\nu = \mu$, we can suppose without loss of generality, with usual meaning of indexing $i = 1, \dots, r_p^-$, that the representants $C_1, \dots, C_{\nu-1}$ chosen are singular primary.

Theorem 3.15. **** On structure of p-class group C_p^-.*

Let $\mathbf{b}_i$ be the ideals defined in relation (10) p. 20. Let $C_p^- = \oplus_{i=1}^{r_p^-} < Cl(\mathbf{b}_i) >$. Let $C_i = \frac{B_i}{\overline{B}_i}$, $\quad B_i\mathbb{Z}[\zeta] = \mathbf{b}_i^p$, $\quad Cl(\mathbf{b}_i) \in C_p^-$, $\quad i = 1, \dots, r_p^-$, where B_i is defined in relation (13) p. 22. Let r_1^- be the degree of the minimal polynomial $P_{r_1^-}(\sigma)$ defined in relation (10) p. 20. With a certain ordering of C_i, $\quad i = 1, \dots, r_p^-$,

1. *C_i are singular primary for $i = 1, \dots, r_p^+$, and C_i are singular not primary for $i = r_p^+, \dots, r_p^-$.*
2. *(a) If $j > i \geq r_p^+ + 1$ then $\mu_j \neq \mu_i$.*
   (b) If $\mu_i = \mu_j$ then $j < i \leq r_p^+$.
3. *$r_p^- - r_p^+ \leq r_1^- \leq r_p^-$.*

Proof.

1. It is an application of a theorem of Furwangler, see Ribenboim [6] (6C) p. 182 and of a theorem of Hecke, see Ribenboim [6] (6D) p. 182.
2. See lemma 3.13 p. 25
3. Apply corollary 3.14 p. 26.

□

3.4.2 π-adic congruences connected to p-class group C_p^+

For $i = r_p^+ + 1, \dots, r_p$, to simplify notations in this lemma, let us note respectively $\mathbf{b}, B$ for ideal $\mathbf{b}_i$ and algebraic integer B_i, as defined in the two relations (10) p. 20 and (14) p. 22.

Theorem 3.16. *****

Let the ideals $\mathbf{b}$, such that $Cl(\mathbf{b}) \in C_p^+$ defined in relation (10) p. 20. There exists $B \in \mathbb{Z}[\zeta]$ such that:

$$(21) \qquad \begin{aligned} &\mu = u_{2n}, \quad 1 \leq n \leq \frac{p-3}{2} \\ &\sigma(\mathbf{b}) \simeq \mathbf{b}^\mu, \\ &B\mathbb{Z}[\zeta] = \mathbf{b}^p, \\ &\sigma(B) = B^\mu \times \alpha^p, \quad \alpha \in \mathbb{Q}(\zeta), \\ &B \equiv 1 \ mod\ \pi^{2n}. \end{aligned}$$

Proof. Similarly to relation (13) p. 22, there exists B with $B\mathbb{Z}[\zeta]=\mathbf{b}^p$ such that

$$\sigma(B)=B^{\mu}\times\alpha^p\times\eta,\quad \alpha\in\mathbb{Q}(\zeta),\quad \eta\in\mathbb{Z}[\zeta+\zeta^{-1}]^*.$$

From relation (32) p. 36, independant forward reference in section dealing of unit group $\mathbb{Z}[\zeta+\zeta^{-1}]^*$, we can write

$$\begin{aligned}
&\eta=\eta_1^{\lambda_1}\times(\prod_{j=2}^{N}\eta_j^{\lambda^j}),\quad \lambda_j\in\mathbf{F}_p,\quad 1\leq N<\frac{p-3}{2},\\
&\sigma(\eta_1)=\eta_1^{\mu}\times\beta_1^p,\quad \eta_1,\beta_1\in\mathbb{Z}[\zeta+\zeta^{-1}]^*,\\
&\sigma(\eta_j)=\eta_j^{\nu_j}\times\beta_j^p,\quad \eta_j,\beta_j\in\mathbb{Z}[\zeta+\zeta^{-1}]^*,\quad j=2,\dots,N,\\
&2\leq j<j'\leq N\Rightarrow \nu_j\neq\nu_{j'},\\
&\nu_j\neq\mu,\quad j=2,\dots,N.
\end{aligned}$$

Let us note

$$E=\eta_1^{\lambda_1},\quad U=\prod_{j=2}^{N}\eta_j^{\lambda_j}.$$

Show that there exists $V\in\mathbb{Z}[\zeta+\zeta^{-1}]^*$ such that

$$\sigma(V)\times V^{-\mu}=U^{-1}\times\varepsilon^p,\quad \varepsilon\in\mathbb{Z}[\zeta+\zeta^{-1}]^*$$

Let us suppose that V is of form $V=\prod_{j=2}^{N}\eta_j^{\rho_j}$. Then, it suffices that

$$\eta_j^{\rho_j\nu_j}\times\eta_j^{-\rho_j\mu}=\eta_j^{-\lambda_j}\times\varepsilon_j^p,\quad \varepsilon_j\in\mathbb{Z}[\zeta+\zeta^{-1}]^*,\quad j=2,\dots,N.$$

It suffices that

$$\rho_j\equiv\frac{-\lambda_j}{\nu_j-\mu}\mod p,\quad j=2,\dots,N,$$

which is possible, because $\nu_j\not\equiv\mu,\quad j=2,\dots,N$. Therefore, for $B'=B\times V$, we get $B=B'V^{-1}$ and so

$$\sigma(B)=\sigma(B'V^{-1})=B^{\mu}\alpha^p\eta=(B'V^{-1})^{\mu}\alpha^p\eta=(B'V^{-1})^{\mu}\times\alpha^p\times E\times U,$$

so

$$\sigma(B')=(B')^{\mu}\sigma(V)V^{-\mu}\times\alpha^p\times E\times U,$$

so

$$\sigma(B')=(B')^{\mu}(U^{-1}\varepsilon^p\times\alpha^p\times E\times U),$$

so we get simultaneously

$$\begin{aligned}
&\sigma(B')=(B')^{\mu}\times\alpha^p\times\varepsilon^p\times E,\quad \alpha\in\mathbb{Q}(\zeta),\\
&\sigma(E)=E^{\mu}\times\varepsilon_1^p,\quad \varepsilon_1\in\mathbb{Z}[\zeta+\zeta^{-1}]^*.
\end{aligned}$$

Show that

$$\sigma(B') = B'^{\mu} \times \alpha'^{p}. \tag{22}$$

1. If $E \in (\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$, then we get

   $$\sigma(B') = B'^{\mu} \times \alpha'^{p}. \tag{23}$$

2. If $E \notin (\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$ then by conjugation σ,

   $$\sigma(B') = (B')^{\mu} \times \alpha_1^p \times E, \quad \alpha_1 \in \mathbb{Q}(\zeta),$$
   $$\sigma^2(B') = \sigma(B')^{\mu} \times E^{\mu} \times b^p, \quad b \in \mathbb{Q}(\zeta),$$

   so gathering these relations

   $$\sigma(B')^{\mu} = (B')^{\mu^2} \times \alpha_1^{p\mu} \times E^{\mu},$$
   $$\sigma^2(B') = \sigma(B')^{\mu} \times E^{\mu} \times b^p,$$

   and so
   $$c^p \times \sigma(B')^{\mu}(B')^{-\mu^2} = \sigma^2(B')\sigma(B')^{-\mu}, \quad c \in \mathbb{Q}(\zeta)$$
   which leads to
   $$c^p B'^{\mu\sigma}(B')^{-\mu^2} = B'^{\sigma^2}(B')^{-\mu\sigma},$$
   and so
   $$(B')^{(\sigma-\mu)^2} = c^p, \quad c \in \mathbb{Q}(\zeta).$$
   Elsewhere $(B')^{\sigma^{p-1}-1} = 1$, so

   $$(B')^{gcd((\sigma^{p-1}-1,(\sigma-\mu)^2)} = (B')^{\sigma-\mu} = \alpha_3^p, \quad \alpha_3 \in \mathbb{Q}(\zeta),$$

   and so $\sigma(B') = (B')^{\mu} \times \alpha_3^p$.

The end of proof is similar to proof of previous lemma 3.10 p. 23. □

3.4.3 π-adic congruences connected to p-class group C_p

Let us consider the ideals $\mathbf{b}_i, \quad i = 1, \dots, r_p$, defined in relation (10) p. 20. Then $Cl(\mathbf{b}_i) \in C_p$. From theorem 3.10 p. 23, and theorem 3.16 p. 27, we can choose the corresponding singular primary number B_i with $B_i\mathbb{Z}[\zeta] = \mathbf{b}_i^p$; then $\sigma(B_i) = B_i^{\mu} \times \alpha_i^p, \quad \alpha_i \in \mathbb{Q}(\zeta), \quad \mu_i = u_{m_i}, \quad 1 \le m_i \le p-2$. Observe that if m_i is odd then $Cl(\mathbf{b}_i) \in C_p^-$ and if m is even then $Cl(\mathbf{b}_i) \in C_p^+$.

The next important theorem **summarize** for all the p-class group C_p the previous theorems 3.9 p. 22 and 3.10 p. 23 for relative p-class group C_p^- and 3.16 p. 27 for p-class group C_p^+ and give explicit π-adic congruences connected to p-class group of $\mathbb{Q}(\zeta)$.

Theorem 3.17. **** π-adic structure of p-class group C_p*

Let the ideals $\mathbf{b}_i, \quad i=1,\dots,r_p$, such that $Cl(\mathbf{b}_i)\in C_p$ and defined by relation (10) p. 20. Then, there exists singular algebraic integers $B_i\in\mathbb{Z}[\zeta], \quad i=1,\dots,r_p$, such that

$$\begin{aligned}
&\mu_i = u_{m_i}, \quad 1\le m_i\le p-2, \quad i=1,\dots,r_p,\\
&\sigma(\mathbf{b}_i)\simeq \mathbf{b}_i^{\mu_i},\\
&B_i\mathbb{Z}[\zeta]=\mathbf{b}_i^p,\\
&\sigma(B_i)=B_i^{\mu_i}\times\alpha_i^p, \quad \alpha_i\in\mathbb{Q}(\zeta),\\
&B_i\equiv 1 \ mod\ \pi^{m_i}.
\end{aligned} \tag{24}$$

Moreover, with a certain reindexing of $i=1,\dots,r_p$:

1. *The r_p^+* **singular** *integers $B_i, \quad i=1,\dots,r_p^+$, corresponding to $\mathbf{b}_i\in C_p^-$ are* **primary** *with $\pi^p \mid B_i-1$.*
2. *The $r_p^- - r_p^+$* **singular** *integers $B_i, \quad i=r_p^++1,\dots,r_p^-$, corresponding to $\mathbf{b}_i\in C_p^-$ are* **not primary** *and verify $\pi^{m_i}\parallel (B_i-1)$.*
3. *The r_p^+* **singular** *numbers $B_i, \quad i=r_p^-+1,\dots,r_p$, corresponding to $\mathbf{b}_i\in C_p^+$ are* **primary** *or* **not primary** *(without being able to say more) and verify $\pi^{m_i}\mid (B_i-1)$.*

Proof.

1. For the case C_p^-, apply lemmas 3.10 p. 23 and theorem 3.15 p. 27. Toward this result, observe also that if B_i is not primary, then $\pi^{2m_i+1}\parallel (B_i')^{p-1}-1$ and so $\pi^{p-1} \not| (B_i')^{p-1}-1$ and $C'=(\frac{B'}{\overline{B'}})^{p-1}$ is not singular primary, therefore B_i' primary $\Leftrightarrow C_i'=\frac{B_i'}{\overline{B_i'}}$ primary.
2. For the case C_p^+ apply the theorem 3.16

$\square$

The case $\mu=u_{2m+1}$ with $2m+1>\frac{p-1}{2}$

In the next lemma 3.18 p. 31 and theorem 3.19 p. 32, we shall investigate more deeply the consequences of the congruence $C\equiv 1 \bmod \pi^{2m+1}$ of lemma 3.9 p. 22 when $2m+1>\frac{p-1}{2}$.

Lemma 3.18. *Let C with $\mu = u_{2m+1}$, $\quad 2m+1 > \frac{p-1}{2}$ written in the form:*

$$C = 1 + \gamma + \gamma_0\zeta + \gamma_1\zeta^u + \cdots + \gamma_{p-3}\zeta^{u_{p-3}},$$
$$\gamma \in \mathbb{Q}, \quad v_p(\gamma) \geq 0, \quad \gamma_i \in \mathbb{Q}, \quad v_p(\gamma_i) \geq 0, \quad i = 0, \dots, p-3,$$
$$\gamma + \gamma_0\zeta + \gamma_1\zeta^u + \cdots + \gamma_{p-3}\zeta^{u_{p-3}} \equiv 0 \ mod\ \pi^{2m+1}, \quad 2m+1 > \frac{p-1}{2}.$$

Then C verifies the congruences

$$\gamma \equiv -\frac{\gamma_{p-3}}{\mu - 1} \ mod\ p,$$
$$\gamma_0 \equiv -\mu^{-1} \times \gamma_{p-3} \ mod\ p,$$
$$\gamma_1 \equiv -(\mu^{-2} + \mu^{-1}) \times \gamma_{p-3} \ mod\ p,$$
$$\vdots$$
$$\gamma_{p-4} \equiv -(\mu^{-(p-3)} + \cdots + \mu^{-1}) \times \gamma_{p-3} \ mod\ p.$$

Proof. We have seen in lemma 3.8 p. 21 that $\sigma(C) \equiv C^\mu \bmod \pi^{p+1}$. From $2m+1 > \frac{p-1}{2}$ we derive that

$$C^\mu \equiv 1 + \mu \times (\gamma + \gamma_0\zeta + \gamma_1\zeta^u + \cdots + \gamma_{p-3}\zeta^{u_{p-3}}) \bmod \pi^{p-1}.$$

Elsewhere, we get by conjugation

$$\sigma(C) = 1 + \gamma + \gamma_0\zeta^u + \gamma_1\zeta^{u_2} + \cdots + \gamma_{p-3}\zeta^{u_{p-2}}. \tag{25}$$

We have the identity

$$\gamma_{p-3}\zeta^{u_{p-2}} = -\gamma_{p-3} - \gamma_{p-3}\zeta - \cdots - \gamma_{p-3}\zeta^{u_{p-3}}.$$

This leads to

$$\sigma(C) = 1 + \gamma - \gamma_{p-3} - \gamma_{p-3}\zeta + (\gamma_0 - \gamma_{p-3})\zeta^u + \cdots + (\gamma_{p-4} - \gamma_{p-3})\zeta^{u_{p-3}}.$$

Therefore, from the congruence $\sigma(C) \equiv C^\mu \bmod \pi^{p+1}$ we get the congruences in the basis $1, \zeta, \zeta^u, \dots, \zeta^{u_{p-3}}$,

$$1 + \mu\gamma \equiv 1 + \gamma - \gamma_{p-3} \bmod p,$$
$$\mu\gamma_0 \equiv -\gamma_{p-3} \bmod p,$$
$$\mu\gamma_1 \equiv \gamma_0 - \gamma_{p-3} \bmod p,$$
$$\mu\gamma_2 \equiv \gamma_1 - \gamma_{p-3} \bmod p,$$
$$\vdots$$
$$\mu\gamma_{p-4} \equiv \gamma_{p-5} - \gamma_{p-3} \bmod p,$$
$$\mu\gamma_{p-3} \equiv \gamma_{p-4} - \gamma_{p-3} \bmod p.$$

From these congruences, we get $\gamma \equiv -\frac{\gamma_{p-3}}{\mu-1} \bmod p$ and $\gamma_0 \equiv -\mu^{-1}\gamma_{p-3} \bmod p$ and then $\gamma_1 \equiv \mu^{-1}(\gamma_0 - \gamma_{p-3}) \equiv \mu^{-1}(-\mu^{-1}\gamma_{p-3} - \gamma_{p-3}) \equiv -(\mu^{-2}+\mu^{-1})\gamma_{p-3} \bmod p$ and $\gamma_2 \equiv \mu^{-1}(\gamma_1 - \gamma_{p-3}) \equiv \mu^{-1}(-(\mu^{-2}+\mu^{-1})\gamma_{p-3} - \gamma_{p-3}) \equiv -(\mu^{-3}+\mu^{-2}+\mu^{-1})\gamma_{p-3} \bmod p$ and so on. □

The next theorem gives an explicit important formulation of C when $2m+1 > \frac{p-1}{2}$.

Theorem 3.19. **** Let $\mu = u_{2m+1}$, $\quad p-2 \geq 2m+1 > \frac{p-1}{2}$, corresponding to C defined in lemma 3.9 p. 22, so $\sigma(C) \equiv C^\mu \bmod \pi^{p+1}$. Then C verifies the formula:*

$$C \equiv 1 - \frac{\gamma_{p-3}}{\mu-1} \times (\zeta + \mu^{-1}\zeta^u + \cdots + \mu^{-(p-2)}\zeta^{u_{p-2}}) \bmod \pi^{p-1}. \tag{26}$$

Proof. From definition of C, setting $C = 1+V$, we get :

$$\begin{aligned}
&C = 1+V,\\
&V = \gamma + \gamma_0\zeta + \gamma_1\zeta^u + \cdots + \gamma_{p-3}\zeta^{u_{p-3}},\\
&\sigma(V) \equiv \mu \times V \bmod \pi^{p+1}.
\end{aligned}$$

Then, from lemma 3.18 p. 31, we obtain the relations

$$\begin{aligned}
&\mu = u_{2m+1},\\
&\gamma \equiv -\frac{\gamma_{p-3}}{\mu-1} \bmod p,\\
&\gamma_0 \equiv -\mu^{-1} \times \gamma_{p-3} \bmod p,\\
&\gamma_1 \equiv -(\mu^{-2}+\mu^{-1}) \times \gamma_{p-3} \bmod p,\\
&\vdots\\
&\gamma_{p-4} \equiv -(\mu^{-(p-3)} + \cdots + \mu^{-1}) \times \gamma_{p-3} \bmod p,\\
&\gamma_{p-3} \equiv -(\mu^{-(p-2)} + \cdots + \mu^{-1}) \times \gamma_{p-3} \bmod p.
\end{aligned}$$

From these relations we get

$$V \equiv -\gamma_{p-3} \times (\frac{1}{\mu-1} + \mu^{-1}\zeta + (\mu^{-2}+\mu^{-1})\zeta^u + \cdots + (\mu^{-(p-2)} + \cdots + \mu^{-1})\zeta^{u_{p-3}}) \bmod p.$$

Then

$$V \equiv -\gamma_{p-3} \times (\frac{1}{\mu-1} + \mu^{-1}(\zeta + (\mu^{-1}+1)\zeta^u + \cdots + (\mu^{-(p-3)} + \cdots + 1)\zeta^{u_{p-3}})) \bmod p.$$

Then

$$V \equiv -\gamma_{p-3} \times (\frac{1}{\mu-1} + \mu^{-1}(\frac{(\mu^{-1}-1)\zeta + (\mu^{-2}-1)\zeta^u + \cdots + (\mu^{-(p-2)}-1)\zeta^{u_{p-3}}}{\mu^{-1}-1})) \bmod p.$$

Then

$$V \equiv -\gamma_{p-3}\times(\frac{1}{\mu-1}+\mu^{-1}(\frac{\mu^{-1}\zeta+\mu^{-2}\zeta^{u}+\cdots+\mu^{-(p-2)}\zeta^{u_{p-3}}-\zeta-\zeta^{u}-\cdots-\zeta^{u_{p-3}}}{\mu^{-1}-1})) \bmod p.$$

Then $-\zeta-\zeta^{u}-\cdots-\zeta^{u_{p-3}}=1+\zeta^{u_{p-2}}$ and $\mu^{-(p-1)}\equiv 1 \bmod p$ implies that

$$V \equiv -\gamma_{p-3}\times(\frac{1}{\mu-1}+\mu^{-1}(\frac{1+\mu^{-1}\zeta+\mu^{-2}\zeta^{u}+\cdots+\mu^{-(p-2)}\zeta^{u_{p-3}}+\mu^{-(p-1)}\zeta^{u_{p-2}}}{\mu^{-1}-1})) \bmod p.$$

Then

$$V \equiv -\gamma_{p-3}\times(\frac{1}{\mu-1})\times(1-(1+\mu^{-1}\zeta+\mu^{-2}\zeta^{u}+\cdots+\mu^{-(p-2)}\zeta^{u_{p-3}}+\mu^{-(p-1)}\zeta^{u_{p-2}})) \bmod p.$$

Then $\frac{1}{\mu-1}+\frac{\mu^{-1}}{\mu^{-1}-1}=0$ and so

$$V \equiv -\gamma_{p-3}\times(\frac{\mu^{-1}}{\mu-1})\times(\zeta+\mu^{-1}\zeta^{u}+\cdots+\mu^{-(p-3)}\zeta^{u_{p-3}}+\mu^{-(p-2)}\zeta^{u_{p-2}}) \bmod p.$$

$\square$

4 On structure of the p-unit group of the cyclotomic field $\mathbb{Q}(\zeta)$

Let us consider the results obtained in subsection 3.4 p.19 for the action of $Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ on C_p^-. In the present section, we assert that this approach can be partially translated *mutatis mutandis* to the study of the p-group of units of $\mathbb{Q}(\zeta)$

$$F = \{\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p\}/ < -1 > .$$

This section contains:

- Some general definitions and properties of the p-unit group F.
- Some π-adic congruences strongly connected to structure of the p-unit-group F. These congruences are of the same kind that those found in previous chapter for p-class group C_p.

4.1 Definitions and preliminary results

- When $h^- \equiv 0 \mod p$, from Hilbert class field theory, there exists *primary* units $\eta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$, so such that

$$\begin{aligned}&\eta \equiv d^p \mod p, \quad d \in \mathbb{Z}, \quad d \not\equiv 0,\\ &\sigma(\eta) = \eta^\mu \times \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta+\eta^{-1}]^*.\end{aligned} \tag{27}$$

- The group $\mathbb{Z}[\zeta+\zeta^{-1}]^*$ is a free group of rank $\frac{p-1}{2}$. It contains the subgroup $\{-1, 1\}$ of rank 1. For all $\eta \in \mathbb{Z}[\zeta+\zeta^{-1}]^* - \{-1, 1\}$

$$\eta \times \sigma(\eta) \times \cdots \times \sigma^{(p-3)/2}(\eta) = \pm 1.$$

Therefore, for each unit $\eta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$, there exists a **minimal** $r_\eta \in \mathbb{N}, \quad r_\eta \leq \frac{p-3}{2}$, such that

$$\begin{aligned}&\eta \times \sigma(\eta)^{l_1} \times \cdots \times \sigma^{r_\eta}(\eta)^{l_{r_\eta}} = \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta+\zeta^{-1}]^*,\\ &0 \leq l_i \leq p-1, \quad i = 1, \dots, r_\eta, \quad l_{r_\eta} \neq 0.\end{aligned} \tag{28}$$

- Let us define an equivalence on units of $\mathbb{Z}[\zeta+\zeta^{-1}]^*$: $\eta, \eta' \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$ are said equivalent if there exists $\varepsilon \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$ such that $\eta' = \eta \times \varepsilon^p$. Let us denote $E(\eta)$ the equivalence class of η.
- We have $E(\eta_a \times \eta_b) = E(\eta_a) \times E(\eta_b)$; the set of class $E(\eta)$ is a group. The group $< E(\eta) >$ generated by $E(\eta)$ is cyclic of order p.

- Observe that this equivalence is consistent with conjugation $E(\sigma(\eta)) = \sigma(E(\eta))$.
- The group $F = \{\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p\}/ < -1 >$ so defined is a group of rank $\frac{p-3}{2}$, see for instance Ribenboim [6] p 184 line 14.
- Similarly to relation (5) p.15, there exists $\eta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$ such that

$$\begin{aligned}
&E(\eta) = E(\eta_1) \times \cdots \times E(\eta_{(p-3)/2}),\\
&E(\sigma(\eta_i)) = E(\eta_i^{\mu_i}), \quad i = 1, \dots, \frac{p-3}{2},\\
&\mu_i \in \mathbb{N}, \quad 1 < \mu_i \le p-1,\\
&F =< E(\eta_1) > \oplus \cdots \oplus < E(\eta_{(p-3)/2}) >,
\end{aligned} \tag{29}$$

  where F is seen as a $\mathbf{F}_p[G]$-module of dimension $\frac{p-3}{2}$.
- For each unit η, there is a minimal polynomial $P_{r_\eta}(V) = \prod_{i=1}^{r_\eta}(V-\mu_i)$ where $r_\eta \le \frac{p-3}{2}$, such that

$$\begin{aligned}
&E(\eta)^{P_{r_\eta}(\sigma)} = E(1),\\
&1 \le i < j \le r_\eta \Rightarrow \mu_i \ne \mu_j.
\end{aligned} \tag{30}$$

- Let $\beta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$. Observe that if $E(\beta) = E(\sigma(\beta))$ then $E(\sigma^2(\beta)) = E(\beta)$ and so $E(1) = E(\beta^{p-1})$ and $E(\beta) = 1$.
- Recall that a unit $\beta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$ is said primary if $\beta \equiv b^p \mod \pi^{p+1}, \quad b \in \mathbb{Z}$.

Lemma 4.1. *Let $\beta \in \mathbb{Z}[\zeta+\zeta^{-1}]^* - (\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$. Then the minimal polynomial $P_{r_\beta}(V)$ is of the form*

$$P_{r_\beta}(V) = \prod_{i=1}^{r_\beta}(V - u_{2m_i}), \quad 1 \le m_i \le \frac{p-3}{2}, \quad r_\beta > 0.$$

Proof. There exists $\eta_1 \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad E(\eta_1) \ne E(1)$, with $E(\eta_1)^{\sigma-\mu_1} = E(1)$. Suppose that $\mu_1^{(p-1)/2} = -1$ and search for a contradiction: we have $E(\eta_1)^{\sigma-\mu_1} = E(1)$, therefore $E(\eta_1)^{\sigma^{(p-1)/2}-\mu_1^{(p-1)/2}} = E(1)$; but, from $\eta_1 \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$, we get $\eta_1^{\sigma^{(p-1)/2}} = \eta_1$ and so $E(\eta_1)^{1-\mu_1^{(p-1)/2}} = E(1)$, or $E(\eta_1)^2 = E(1)$, so $E(\eta_1)^2$ is of rank null and therefore $E(\eta_1) = E(\eta_1^2)^{(p+1)/2}$ is also of rank null, contradiction. The same for $\mu_i, \quad i = 1, \dots, r_\beta$. $\square$

4.2 π-adic congruences on p-unit group F of $\mathbb{Q}(\zeta)$

The results on structure of relative p-class group C_p^- of subsection 3.4 p. 19 can be translated to some results on structure of the group F: from $\eta_i^{p-1} \equiv 1 \bmod \pi$ and from $< E(\eta_i^{p-1}) >=< E(\eta_i) >$, we can always, without loss of generality, choose the determination η_i such that $\eta_i \equiv 1 \bmod \pi$. We have proved that

$$\begin{aligned} &\eta_i \equiv 1 \bmod \pi, \\ &\sigma(\eta_i) \equiv \eta_i^{\mu_i} \bmod \pi^{p+1}. \end{aligned} \tag{31}$$

Then, starting of this relation (31), similarly to lemma 3.9 p. 22 we get:

π-adic congruences of unit group $F = \{\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p\}/ < -1 >$
This theorem summarize our π-adic approach on group of p-units F.

Theorem 4.2. **** With a certain ordering of index $i = 1, \dots, \frac{p-3}{2}$, there exists a fundamental system of units η_i, $\quad i = 1, \dots, \frac{p-3}{2}$, of the group $F = \{\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p\}/ < -1 >$ verifying the relations:*

(32)

$$\eta_i \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad i = 1, \dots, \frac{p-3}{2},$$

$$\mu_i = u_{2n_i}, \quad 1 \leq n_i \leq \frac{p-3}{2}, \quad i = 1, \dots, \frac{p-3}{2},$$

$$\sigma(\eta_i) = \eta_i^{\mu_i} \times \varepsilon_i^p, \quad \varepsilon_i \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad i = 1, \dots, \frac{p-3}{2},$$

$$\sigma(\eta_i) \equiv \eta_i^{\mu_i} \ \mathit{mod}\ \pi^{p+1}, \quad i = 1, \dots, \frac{p-3}{2},$$

$$\pi^{2n_i} \parallel \eta_i - 1, \quad i = 1, \dots, r_p^+, \quad \eta_i \ \textit{not primary},$$

$$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i > 0, \quad i = r_p^+ + 1, \dots, r_p^-, \quad \eta_i \ \textit{primary}.$$

$$\pi^{a_i(p-1)+2n_i} \parallel \eta_i - 1, \quad a_i \in \mathbb{N}, \quad a_i \geq 0, \quad i = r_p^- + 1, \dots, r_p, \quad \eta_i \ \textit{primary or not primary}$$

$$\pi^{2n_i} \parallel \eta_i - 1, \quad i = r_p + 1, \dots, \frac{p-3}{2}, \quad \eta_i \ \textit{not primary}.$$

Proof.

1. We are applying in this situation the same π-adic theory to p-group of units $F = \mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$ than to relative p-class group C_p^- in subsection 3.4 p. 19, with a supplementary result for units due to Denes, see Denes [1] and [2] and Ribenboim [6] (8D) p. 192.

2. Similarly to decomposition of components of C_p in singular primary and singular not primary components, the rank $\frac{p-3}{2}$ of F has two components ρ_1 and $\frac{p-3}{2}-\rho_1$ where ρ_1 corresponds to the maximal number of independant units η_i primary and $\rho_2=\frac{p-3}{2}-\rho_1$ to the units η_i not primary.

□

The next lemma for the unit group $\mathbb{Z}[\zeta+\zeta^{-1}]^*$ is the translation of similar lemma 3.13 p. 25 for the relative p-class group C_p^-.

Lemma 4.3. **** Let η_1,η_2 defined by relation (32) p. 36. If $\mu_1=\mu_2$ then $\eta_1\times\eta_2^{-1}$ is a primary unit.*

The group $F=\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$ can be written as the direct sum $F=F_1\oplus F_2$ of a subgroup F_1 with ρ_1 primary units (p-rank ρ_1 of F_1) and of a subgroup F_2 with $\rho_2=\frac{p-3}{2}-\rho_1$ fundamental not primary units (p-rank ρ_2 of F_2): towards this assertion, observe that if η_1 and η_2 are two not primary units with $\sigma(\eta_1)\times\eta_1^{-\mu}\in(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$ and $\sigma(\eta_2)\times\eta_2^{-\mu}\in(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$ then $\eta_1\times\eta_2^{-1}$ is a primary unit and it always possible to replace $\{\eta_1,\eta_2\}$ by $\{\eta_1\times\eta_2^{-1},\eta_2\}$ in the basis of F, so to *push* all the primary units in F_1 and to make the set F_2 of not primary units as a group. Observe that ρ_1 can be seen also as the maximal number of independant primary units in F.

Structure theorem of unit group $F=\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p$

Theorem 4.4. *****

Let r_p^- be the relative p-class group of $\mathbb{Q}(\zeta)$. Let r_p^+ be the p-class group of $\mathbb{Q}(\zeta+\zeta^{-1})$. Let ρ_1 be the number of independant primary units of F. Then

$$r_p^- - r_p^+ \le \rho_1 \le r_p^-. \tag{33}$$

Proof. We apply Hilbert class field theory: for a certain order of the indexing of $i=1,\dots,\frac{p-3}{2}$:

1. There are exactly r_p^+ independant unramified cyclic extensions

$$\mathbb{Q}(\zeta,\omega_i)/\mathbb{Q}(\zeta),\quad \omega_i^p\in\mathbb{Z}[\zeta+\zeta^{-1}]-\mathbb{Z}[\zeta+\zeta^{-1}]^*\quad i=1,\dots,r_p^+.$$

2. There are exactly $r_p^- - r_p^+ = r_p^-$ independant unramified cyclic extensions

$$\mathbb{Q}(\zeta,\omega_i)/\mathbb{Q}(\zeta),\quad \omega_i^p\in\mathbb{Z}[\zeta+\zeta^{-1}]^*,\quad i=r_p^+ +1,\dots,r_p^-.$$

3. There is a number n on independant unramified cyclic extensions witn $0 \leq n \leq r_p^+$ with

$$\mathbb{Q}(\zeta, \omega_i)/\mathbb{Q}(\zeta), \quad \omega_i^p \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad i = r_p^- + 1, \dots, r_p.$$

4. There are no independant unramified cyclic extensions with

$$\mathbb{Q}(\zeta, \omega_i)/\mathbb{Q}(\zeta), \quad \omega_i^p \in \mathbb{Z}[\zeta+\zeta^{-1}]^*, \quad i = r_p + 1, \dots, \frac{p-3}{2}.$$

□

The case $\mu = u_{2n}$ with $2n > \frac{p-1}{2}$

In the next theorem we shall investigate more deeply the consequences of the congruence $\eta_i \equiv 1 \bmod \pi^{2n_i}$ when $2n_i > \frac{p-1}{2}$. We give an explicit congruence formula in that case. To simplify notations, we take η, μ, n for η_i, μ_i, n_i. The next theorem for the p-unit group $F = \{\mathbb{Z}[\zeta+\zeta^{-1}]^*/(\mathbb{Z}[\zeta+\zeta^{-1}]^*)^p\}/ < -1 >$ is the translation of similar theorem 3.19 p. 32 for the relative p-class group C_p^-.

Theorem 4.5. **** Let $\mu = u_{2n}, \quad p-3 \geq 2n > \frac{p-1}{2}$, corresponding to $\eta \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$ defined in relation (32) p. 36, so $\sigma(\eta) = \eta^\mu \times \varepsilon^p, \quad \varepsilon \in \mathbb{Z}[\zeta+\zeta^{-1}]^*$. Then η verifies the explicit formula:*

$$(34) \qquad \eta \equiv 1 - \frac{\gamma_{p-3}}{\mu - 1} \times (\zeta + \mu^{-1}\zeta^u + \dots + \mu^{-(p-2)}\zeta^{u_{p-2}}) \ mod\ \pi^{p-1}, \quad \gamma_{p-3} \in \mathbb{Z}.$$

References

[1] P. Dénes, *Uber irregulare Kreiskorper*, Publ. Math. Debrecen, 3, 1954, pp. 17-23.

[2] P. Dénes, *Uber Grundeinheitssysteme der irregularen Kreiskorper von besonderen Kongruenzeigenschaften*, Publ. Math. Debrecen, 1954, pp. 195-204.

[3] P. Dénes, *Uber den zweiten Faktor der Klassenzahl und den Irregularitatsgrad der irregularen Kreiskorper*, Publ. Math. Debrecen, 4, 1956, pp. 163-170.

[4] P. Furtwangler, *Allgemeiner Existenzbeweis fur den Klassenkorper eines beliebigen algebraischen Zallkorpers*, Math Annalen, 63, 1907, 1-37.

[5] E. Hecke, *Uber nicht-regulare Primzahlen und der Fermatschen Satz*, Nachr Akad. d. Wiss. Gottingen, 1910, 429-434.

[6] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[7] K. Ribet, *A modular construction of unramified* $p-$*extensions of* $\mathbb{Q}(\mu_p)$., Invent.Math. no 34, 1976, pp. 151-162.

[8] L. Stickelberger *Uber eine Verallgemeinerung der Kreistheilung*, Math. Annal., 37 , 1890, pp 321-367.

[9] L.C. Washington, *Introduction to cyclotomic fields*, Springer, 1996.

Roland Quême
13 avenue du château d'eau
31490 Brax
France
2005 fev 04
tel : 0033561067020
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/